

DEBILIDAD INFORMÁTICA EN LOS GOBIERNOS MUNICIPALES. UNA PRIORIDAD PENDIENTE DEL DESARROLLO LOCAL

Emilio Velazco Gamboa (*)

Jorge David Romero Cortés (**)

Fecha de publicación: 01/07/2012

1. Introducción

Cuántas películas de acción y de ciencia ficción no habremos visto con temas en los que niños y adolescentes invaden los sistemas informáticos de grandes empresas y corporaciones, causando estragos en la economía de estas así como en la de su país y aun en la economía mundial. O bien, de adolescentes que burlan los sistemas de defensa de naciones poderosas como los Estados Unidos y ponen, en un juego de guerra, al mundo entero a punto de una conflagración nuclear.

Pues bien: esas tramas ficticias hoy son una realidad preocupante. Expertos en sistemas computacionales se la pasan entrando y saliendo de las computadoras de millones de usuarios de la red de redes, así como de las computadoras de empresas, industrias y hasta dependencias de gobierno, con una impunidad prácticamente total ante la ausencia de métodos efectivos de seguridad para sus máquinas.

Año con año, las corporaciones privadas, las instituciones académicas, e incluso numerosos organismos sociales invierten grandes cantidades en firewalls (muros virtuales contra intrusos), antivirus, antispyware (esquemas contra software espía) y antimalware (esquemas contra software dañino, etc.). Desafortunada-mente, muchos organismos gubernamentales no tienen esas prevenciones, y conforme es más básico su nivel funcional, menos las poseen.

(*) Politólogo | Máster en Derecho y en Sociología
emiliovelazco@hotmail.es | emiliovelazco@hotmail.com

(**) Doctor en Administración Pública | Doctorando en Derecho.

Es decir, en el gobierno federal y los demás poderes hay recursos económicos fuertes y una gran infraestructura de servicios, lo que les ha permitido adquirir herramientas costosas pero sumamente poderosas para combatir la presencia de hackers y demás delincuentes informáticos. Los gobiernos estatales también son fuertes económicamente, aunque menos que el gobierno federal. Pero como sea, en lo general se han podido precaver de estos ataques, o al menos, atenuar un poco sus efectos.

Pero en los ayuntamientos –y más en los ayuntamientos de los municipios latinoamericanos, aunque los habrá en España y Portugal que tampoco sean muy fuertes económicamente– la situación es diferente. Municipios grandes, con gobiernos locales cuya situación financiera es un poco más favorable, con mejores recursos, con mayores aportaciones estatales y federales, quizá pueden costear la adquisición y mantenimiento de sistemas anti intrusión con todo lo que implica en personal, gastos directos (software, hardware, equipo auxiliar) y gastos indirectos (electricidad, insumos).

Así, hay gobiernos municipales cuya captación y recursos son muchísimo menores que los de otras grandes ciudades iberoamericanas ya sea por su marginación, mínima densidad poblacional, bajos índices de desarrollo, escasa inversión y fuentes de empleo, etc. (esas ciudades constituyen la mayoría del universo de municipios iberoamericanos) También, hay ciudades que suelen ser segundo o tercer lugar en importancia y poderío económico en las provincias y en las que, no obstante, su captación de ingresos no es tan alta. Finalmente, hay ciudades que tienen dimensiones territoriales y demográficas menores que las grandes capitales provinciales, y que sin embargo, son autosuficientes económicamente.

Sin embargo, y pensando en los municipios con menor capacidad en recursos financieros y en los que pueden enseñorearse los criminales virtuales, ¿cuál es el riesgo o riesgos a los que se potencialmente se enfrentan estos gobiernos locales menos poderosos económica y tecnológicamente, ante hackers y otros delincuentes informáticos y tecnológicos definitivamente mejor preparados y pertrechados? Analicemos la situación y tratemos de responder a esta pregunta.

2. Antecedentes: hackeo y delincuencia virtual

“Hacker es el neologismo utilizado para referirse a un experto en varias o alguna rama técnica relacionada con la informática: programación, redes de computadoras, sistemas operativos, hardware de red/voz, etc. Se suele llamar hackeo y hackear a las obras propias de un hacker”¹. Claudio

¹ *Hacker* En *Wikipedia*: <http://es.wikipedia.org/wiki/Hacker> (Fecha de consulta: 12 de enero de 2012).

Hernández, de la Universidad de Guadalajara, dice que la ley e incluso los medios escritos aluden a los expertos de la informática y la programación que lindan con lo ilegal, y dice que “en la actualidad, se describe a estos personajes como auténticos expertos en sistemas digitales que disfrutaban explorando sistemas y probando sus capacidades en oposición a los simples usuarios”².

Es preciso aclarar que el término "hackers" trasciende a los expertos relacionados con la informática, para también referirse a cualquier profesional que está en la cúspide de la excelencia en su profesión, ya que en la descripción más pura, un hacker es aquella persona que le apasiona el conocimiento, descubrir o aprender nuevas cosas y entender el funcionamiento de éstas. Sin embargo, se suele relacionar más al hacker y al hackeo (en inglés, *hacking*) con una serie de delitos bien definidos de corte informático. “Se dice que el término de hacker surgió de los programadores del Instituto Tecnológico de Massachussets (MIT), que en los 60, por usar hacks, se llamaron a sí mismos *hackers* para indicar que podían hacer programas mejores y aún más eficaces, o que hacían cosas que nadie había podido hacer”.

Ahora bien, ¿qué es un hack? Se ha consultado, para este ensayo, a Wikipedia, a falta de otras fuentes considerables como “oficiales”, pues pese a la popularidad del término, ni los diccionarios suelen contener estas palabras nuevas, o neologismos, como es el término correcto, las definen. Pues bien, defínase la expresión “hack”. “Un **hack** (en inglés recortar) es la palabra utilizada en determinados sectores de las tecnologías para denominar a las pequeñas modificaciones que se le pueden hacer a un programa o máquina para mejorar o alterar su funcionamiento, particularmente si se trata de una solución creativa o poco convencional a un problema”³.

También, agrega esta fuente, se dice que la palabra deriva de "hack", "hachar" en inglés, término que se utilizaba para describir la forma en que los técnicos telefónicos arreglaban cajas defectuosas, un golpe seco. Y la persona que hacía eso era llamada hacker. En cualquier caso, la vox pópuli –y por desgracia, también la voz de muchos ignorantes que se dedican a mal informar a través de medios de comunicación masiva– se ha dado en denominar *hacker* a los delincuentes informáticos, por lo que, en estos tiempos, se identifica de facto y automáticamente a los hackers con la odiosa y repudiada figura de la criminalidad, especialmente, con la delincuencia organizada.

² Hernández, C. (2001). *Hackers. Los piratas del chip y de Internet*. Guadalajara: Universidad de Guadalajara, p. 34.

³ *Hack*. En *Wikipedia*: <http://es.wikipedia.org/wiki/Hacks> (Fecha de consulta: 12 de enero de 2012).

3. El hackeo a instancias oficiales, un panorama general

El espacio para hablar de los daños causados por hackers a la economía de las ciudades, de muchos países y aún del mundo, sería largo y requeriría muchos detalles. Conocemos muchos casos y sabemos que se han perdido millones de dólares como resultado de los daños provocados por los piratas y delincuentes de las ciencias telemáticas. Asumamos, pues, por un momento, que conocemos este problema aun cuando no sea al detalle. ¿Qué pasa con el hackeo oficial? Por el momento, denominemos hackeo oficial a los ataques que piratas y delincuentes informáticos cometen contra portales electrónicos –informativos, de trámites y de servicios, de consulta, entre otros– y sitios Web de dependencias de los poderes que dirigen la función gubernativa de un país o localidad.

En el caso de México, se hablaría de los poderes federales, de los poderes de las entidades federativas, y de los gobiernos municipales. Pero esta situación no es nueva, pues en México ya se han dado varios casos de hackeo oficial. Sin embargo, y dada la magnitud de las dependencias atacadas, se mencionan algunos casos, por sí mismos paradigmáticos: el hackeo a la página electrónica del Gobierno del Estado de Tabasco y a la de la Cámara de Senadores. Sobre el caso de Tabasco se tiene la siguiente información de conocimiento público, presentada a modo de crónica⁴:

- “La página de Internet del gobierno del estado de Tabasco fue atacada la mañana de este lunes” –del lunes 18 de agosto de 2008) “por hackers que sustituyeron la información de la administración estatal por una fotografía a color de la Chilindrina y un mensaje contra la privatización de Pemex, contra la violencia en el país y contra el narcotráfico”.
- “El sitio <http://www.tabasco.gob.mx> aparecía con problemas técnicos hacia las 10:00 horas de hoy. Sin embargo, al dar click en el link de Sala de Prensa, (www.tabasco.gob.mx/sala_prensa) aparecía hasta las 10:34 un fondo negro con una fotografía del personaje de la Chilindrina y un mensaje de los 'hackers'. Hacia las 11:25 horas, los servicios de la página del gobierno estatal quedaron restaurados”.

Por su parte, el Senado de la República también fue hackeada ya el 9 de mayo de 2008. El diario *El Universal* dio la siguiente crónica⁵:

- La página de internet del Senado de la República fue 'hackeada' por gente que se identifica como los "informáticos" del Gob y Suckean, de Argentina y Chile para el mundo.

⁴ Hackean página web del gobierno de Tabasco (Fecha de publicación: Lunes, 18 de agosto de 2008). Periódico electrónico “Tabasco hoy”. http://www.tabascohoy.com.mx/nota.php?id_notas=161036

⁵ Zárate, A. (Fecha de publicación: Viernes, 9 de mayo de 2008). 'Hackean' página de Internet del Senado. Versión electrónica del diario *El Universal*. <http://www.el-universal.com.mx/notas/505467.html>

- En lugar de la página que describe las actividades de los senadores, lo que aparece es una fotografía de la Chilindrina a color con sus lentes y pecas, pero también sobresale una leyenda que se pronuncia en contra de la privatización de Pemex y que le manda un mensaje al presidente Calderón que dice: "Deja mx en paz y deja de explotar a la gente". Remata con la expresión "Es (un honor estar con obrador!!!!) ANarquía - Jamz".
- Además, debajo de la foto aparece en inglés una leyenda que dice que la página ha cambiado de dueño y sin faltar la expresión "¡Chanfle!" característica del personaje creado por el comediante mexicano Roberto Gómez Bolaños.
- Los hackers envían un saludo al comediante y le dicen que todavía lo ven todas las mañanas, porque es lo más grande que existe.
- También envían saludos a personajes con seudónimos que parecieran ser de diferentes países. Después aparecen mensajes dirigidos a Argentina y México, en el primer caso en relación a los problemas del campo, y en el segundo su rechazo a la privatización de Petróleos Mexicanos. Para terminar, los hackers ponen sus correos electrónicos.

Cierto o no que defienden al petróleo, que están apoyando la lucha de Andrés Manuel López Obrador, que están contra la globalización, e independientemente de cualquier causa que puedan tener, muchos hackers han cometido violaciones contra la intimidad de millones de usuarios en la red, así como contra gobiernos y dependencias, pero sobre todo, y en el caso que interesa a este artículo, contra el público que depende de trámites y servicios por Internet. En otro caso, el Senado de México –junto con otros portales en este y otros países– fue atacado por Anonymous el 28 de enero de 2012 en uno de los numerosos actos protesta que este grupo llevó a cabo en 2011 y 2012 contra las numerosas medidas adoptadas en México y otros países para restringir los derechos de los internautas al libre intercambio de archivos e información en la red de redes –entre ellas las famosas leyes ACTA y SOPA–.

El mismo grupo atacó a numerosos portales electrónicos, entre ellos el de la página de la Arquidiócesis de México el 19 de marzo de 2012 y, en fechas más recientes, el del Partido Revolucionario Institucional (PRI) el 19 de mayo del mismo año. Ahora bien, estos ataques cometidos contra el Senado en las dos ocasiones reportadas, contra la Arquidiócesis, contra el gobierno de Tabasco en 2008 y el del PRI en 2012 no produjeron daños; sólo fueron protestas aisladas al mismo tiempo que demostraciones de superioridad de parte de los hackers. Pero, ¿qué pasaría si otros

piratas/delincuentes virtuales deciden causar un daño real a las dependencias y gobiernos?

4. Riesgos potenciales del hackeo a páginas oficiales

Los escenarios son muchos y el espacio para este ensayo es breve, pero vayamos a una de las aristas que más dolores de cabeza podrían provocar si un hacker decide causar daño a las instituciones públicas invadiéndolas. Definitivamente, me atrevo a pensar que dicha arista podría ser la de los servicios que el gobierno presta o facilita vía Internet. Repasemos un poco las generalidades de los servicios públicos. Para el Doctor Andrés Serra Rojas, los servicios públicos pueden clasificarse en cuatro grandes categorías si se parte de la competencia de los diversos órganos del Estado mexicano⁶:

- a) Servicios públicos federales;
- b) Servicios públicos de las entidades federativas;
- c) Servicios públicos municipales, y
- d) Servicios públicos internacionales.

Con base en su observación, algunos especialistas han logrado ubicar las siguientes áreas de servicios públicos que prestan federación y estados⁷:

- 1) Seguridad pública, y en el caso del gobierno federal, seguridad pública y defensa nacional. También puede contarse la labor de protección civil dentro de este rubro.
- 2) Comunicaciones y transportes.
- 3) Salud.
- 4) Asistencia pública.
- 5) Deporte, recreación y cultura.
- 6) Procuración de justicia.
- 7) Servicios administrativos y fiscales (entre los que destacan la administración tributaria, finanzas públicas, reglamentos, registro del servicio militar, etc.).

Para el Maestro Arturo Pontifes⁸, existen las siguientes tipologías de los servicios públicos:

⁶ Serra Rojas, A. (1994). *Derecho administrativo*, primer curso. México: Porrúa, p. 113.

⁷ Velazco Gamboa, E. (Noviembre de 2003). *La pobreza en México y su combate*. Tesis de Licenciatura en Ciencias Políticas. Puebla: Universidad del Desarrollo del Estado de Puebla, pp. 50-52.

⁸ Pontifes Martínez, A. (2008). *Concepto, características y modalidades de operación de los servicios públicos municipales*. Ponencia del Módulo IV “Servicios públicos municipales” del Diplomado en Desarrollo Local y Planeación Municipal Participativa impartido durante los meses de Mayo a Octubre de 2008. México: INAFED-INDESOL-UAMX, p. 9.

- a) Por su carácter material.
- b) Por la instancia provisora.
- c) Clasificación económica.
- d) Clasificación doctrinaria.
- e) Clasificación urbanística.

Muchos de estos servicios pueden ser accedidos por medio de páginas donde se realizan trámites, sean gratuitos o con algún costo, tales como la gestión e impresión de la Cédula Única del Registro de Población (CURP), el acta de nacimiento, el pago impuesto predial, etc. En otros portales, por ejemplo, la Secretaría de Hacienda y Crédito Público recauda el pago de contribuciones. Asimismo, hay ayuntamientos que prestan servicios a través de portales electrónicos. Si un hacker, por diversión, por anarquía, o por simples deseos de fastidiar, provoca un caos en esas páginas, podría causar no sólo un problema administrativo y de gestión, sino incluso lograr la deslegitimación de un gobierno.

Si a ello le sumamos las pérdidas económicas que un gobierno local podría sufrir, así como las que el público ciudadano tendría que padecer, el orden de gobierno podría romperse y traer con ello, además, la demostración de superioridad de los delincuentes virtuales, quienes, reafirmados en su poderío, no tardarían en buscar objetivos más grandes para producir averías mayores. La rebeldía de grupos como Anomymous quedaría como un juego de niños y demostraría que su intención no era causar perjuicios; sólo que, para entonces, los daños de los verdaderos criminales serían incalculables y, quizá, irreparables...

5. Reflexión final

La debilidad informática en los gobiernos municipales es una prioridad pendiente del desarrollo local por cuanto puede llegar a cimbrar las estructuras financieras, políticas, de gestión, de administración y de servicios. Ello se puede deber a la insuficiencia de recursos para adquirir el servicio de protección informática en todo lo que conlleva. Pero también se debe a la falta de previsión, visión y preparación de los detentadores del poder en el ámbito municipal. Si no se conoce un riesgo, o no se tiene conciencia plena de éste, o si teniéndola se le menosprecia, se pueden cometer errores cuyas consecuencias pueden ser descomunales, sobre todo, en lo que concierne al bien común y al servicio al público.

Estamos a tiempo de prever. Mañana, podríamos amanecer no con la imagen de La Chilindrina en pantalla, o con la novedad de que se cayó el portal de un partido político con fama bien ganada de represor, o de una instancia religiosa que, en casos como el de México, se comporta de una

forma medieval, sino con la noticia de que el caos ha dejado de ser un supuesto producido por la imaginación popular o por la imaginación de escritores febriles, para convertirse en una noticia de dimensiones desagradables y colosales.