Sin dudas, MICROSOFT SPY (16/09/04)

Estimados Internautas:

Creo que con estos artículos queda por demás claro que Microsoft ó el Gobierno de Estados Unidos espía a los usuarios de Windows.
Este es uno de los puntos fundamentales para que cada vez más gobiernos opten por el software libre.
El poder tener acceso al código de los programas es fundamental para cuando se maneja información crítica, ya que con el código se sabe lo que hace el sistema y se puede mejorar o adaptar, según las necesidades.
Cada usuario es libre de optar por el sistema que desee, pero para que esa libertad de elección sea verdadera debe saber cuales son las consecuencias de su elección, ó a que debe renunciar según la elección hecha. Si elige Windows, renuncia a su privacidad.
Adjunto los artículos con los links respectivos.
Espero que sea de su interés, y los difundan en sus ámbitos.
Quedo abierto a las críticas, las cuales serán publicadas en la sección "Comentarios"
Saludos.
Kbza

El último escándalo de Microsoft

En entrevista con Qué Pasa, el canadiense Andrew Fernandes explica cómo descubrió una segunda clave en los programas Windows, que permitiría a la Agencia de Seguridad estadounidense acceder a las bases de datos de cualquier computador del mundo.
http://www.quepasa.cl/revista/1484/38.html

La semana pasada Microsoft volvió a ocupar los titulares de la prensa internacional. Esta vez no por el tema del monopolio, sino por un descubrimiento que perturbó a quienes utilizan el programa Windows (cerca del 95 % de los computadores en el mundo). Mientras realizaba su trabajo de rutina como programador de computadores, Andrew Fernandes, Director Científico de la Cryptonym Corporation, en Ontario, Canadá, descubrió lo que podría llamarse una "puerta trasera" de acceso al sistema Windows NT. Se trata de una clave de entrada, distinta a la original, y que también serviría para ingresar sin autorización a los programas Windows 95, 98 y 2000 en computadores de cualquier parte del mundo. Lo que más sorprendió al experto fue que dicha clave tuviera el nombre de "NSA", sigla de la Agencia de Seguridad Nacional de Estados Unidos, organismo que, entre otras cosas, revisa y autoriza la exportación de todos los softwares.
La preocupación de la NSA no es el producto en sí, sino el sistema de encriptación que provee, es decir, la posibilidad de codificar la información para impedir que sea comprendida por otros, que no tienen la clave de acceso para decodificarla. Hasta 1996, el gobierno de Estados Unidos consideraba ilegal la exportación de sistemas de encriptación de más de 40 bit (una clave de 8 bits tiene 256 valores posibles), por considerarlos difíciles de romper. En la actualidad, la NSA permite la salida de sistemas que tienen encriptaciones de hasta 56 bit (con 72 trillones de posibles combinaciones). Pero las preocupaciones de la NSA resurgieron hace poco, puesto que la criptografía de 128 bit comienza a ser el nuevo estándar para la encriptación de datos.
Sobre las razones que Microsoft habría tenido para agregar una segunda clave de acceso a su programa Windows y las posibles consecuencias para los usuarios, Andrew Fernándes conversó telefónicamente con la periodista de Qué Pasa, Francisca De la Paz.
- ¿Cómo descrubrió "la puerta trasera" de Windows?.
- Fue por error, mientras trabajaba en un problema de programación usando Windows NT. Sucedieron algunas cosas extras y, entre accidentes y errores, caí en la clave "NSAKEY".
Accidentalmente apareció en mi pantalla.
- En palabras simples, ¿qué es la "puerta trasera" de Windows?.
- Windows da al usuario, junto con varios otros, servicios para usar encriptación de datos (codificación, en cifras, de la información que se almecena en el computador). Para ello, desarrolla modelos computacionales llamados Servicios Proveedores de Criptografía (CSP). Lo que hace esta puerta trasera es permitir a alguien distinto de Microsoft, posiblemente la NSA, poner su propio CSP en Windows.
- ¿La NSA podría decodificar datos de los computadores que usan Windows?.
- La segunda clave en Windows sólo permite a quienes la poseen -hasta ahora presumiblemente la NSA- cargar un servicio de criptografía en Windows. Es decir, controlar las funciones de encriptación de datos. Esto no les da acceso inmediato a todos los datos encriptados en el computador, pero sí hace que las máquinas sean más vulnerables a la penetración no autorizada en el sistema. La "puerta trasera" permite cargar un programa capaz de vulnerar la criptografía de Windows. Quizás ni siquiera tenga que decodificar nada, basta con interceptar los datos antes de que sean encriptados.

- ¿Que lo hace pensar que esta "llave" es para la Agencia de Seguridad Nacional de Estados Unidos? ¿No podría ser un alcance de nombres?.
- En criptografía, la sigla "NSA" sólo significa una cosa: National Security Agency . Si esa sigla apareciera en cualquier otro lugar de Windows, no habría nada de que sospechar, porque podría significar cualquier cosa. Sin embargo, NSA aparece justo dentro de su modelo para la encriptación de datos. Por eso la conexión es con la NSA y no otra cosa.
- ¿Por qué la NSA desearía tener acceso al programa Windows?.
- Por muchos motivos, si se considera cómo funciona el espionaje industrial, por ejemplo. Aunque no existiera esta puerta trasera, de igual forma se podría entrar a Windows, claro que ella permite hacerlo mucho más fácilmente. La existencia de esta segunda clave no implica una falla total en Windows, pero sí un vacío en su sistema de seguridad.
- Microsoft asegura que es sólo una clave de respaldo.
- Podría serlo, pero eso no tiene sentido. Técnicamente no te sirve de nada tener una segunda clave, porque cuando la original se ve compormetida, no se puede revocar. Es decir, si la primera clave está afectada, lo estará todo el sistema aunque exista una clave de respaldo. Microsoft debería saber esto, porque en la compañía trabajan muchos metamáticos y expertos en criptografía. Además, si efectivamente fuera una clave de respaldo, por qué tiene que llamarse "NSA". Pudieron haber buscado otro nombre, como "Clave 2" o "Clave de Respaldo". Y no fue así, la clave que ellos aseguran es de respaldo se llama claramente "NSAKEY".
- ¿La existencia de una "puerta trasera" para Windows puede afectar el resto de las aplicaciones del programa, como el correo electrónico o el acceso a Internet?.
- Depende de si el programa quiere o no usar criptografía. Lo más común es que el software realice por sí mismo la encriptación de datos. Pero también está la opción de que Windows la haga y esto sería un peligro. Ahora, no hay que olvidar que Windows tiene muchos "bichos" (pequeñas fallas que debilitan la seguridad del sistema) en los servicios que ofrece. Se han descubierto "bichos" en Internet Explorer 4, en Internet Explorer 5 y en el programa Java. Este tipo de fallas es que el permitió, hace poco, la entrada de hackers a las casillas de correo que Microsoft ofrece a través de Hotmail.
- ¿Quiénes deberían estar preocupados?.
- Quienes operan grandes centros de bases de datos que necesitan fuertes sistemas de seguridad. Como los bancos, las grandes empresas o las organizaciones gubernamentales.
- ¿Qué pasa con el usuario común?.
- Microsoft tiene pésima reputación en el tema de seguridad y de programación de los distintos softwares que ofrece en Windows. Por ejemplo, las fallas en la aplicación Microsoft Outlook podrían hacer que un virus que llegó al computador a través de Internet afectara todas las otras aplicaciones. Esto no tiene nada que ver con la NSA, sino con una mala programación de los softwares por parte de Microsoft. El usuario común debería estar preocupado de los virus computacionales que viajan por Internet. Ese tipo de cosas son las que pueden afectar su sistema y no el espionaje que podría estar llevando a cabo la NSA.
- La NSA no permite la exportación de softwares con fuertes servicios de criptografía. ¿Piensa que a cambio de que le permitieran exportar Windows, Microsoft accedió a "debilitar" su sistema de seguridad a través de una clave para la agencia?.
- Buena pregunta. La criptografía implica hablar en códigos. Un código débil es un sistema que puede ser fácilmente interpretado por otra persona. Por ejemplo, si comenzáramos a hablar en alemán y alguien nos está escuchando sería un código débil, porque bastaría con tomar un diccionario de alemán o contactar a alguien que hablara el idioma para decodificar lo que decimos. En computación es lo mismo. Si el computador puede adivinar el código fácilmente, la criptografía es débil. Ahora, cuando la criptografía es fuerte, el computador más rápido del planeta podría tardar miles de millones de años en descifrar el código. Por ello, la razón oficial que da el gobierno norteamericano para no permitir la exportación de programas que usan criptogtrafía fuerte es para "el refuerzo de la ley"; es decir, para evitar que actividades ilegales -como el tráfico drogas, el lavado de dinero, los planes de organizaciones criminales o terroristas- se realicen a través de comunicaciones encriptadas imposibles de descrifar.
- ¿Y qué tuvo que hacer Microsoft para exportar su programa Windows?.
- En Estados Unidos, para obtener el permiso de exportación hay que obtener la autorización del Departamento de Comercio. Sin embargo, este departamento no da el visto bueno a ningún software que no haya pasado previamente por la revisión técnica de la NSA.
- ¿Puede eliminarse la "puerta trasera"?
- Técnicamente se puede, pero sería ilegal. Yo tengo algunos softwares capaces de hacerlo, pero no puedo vender programas que permitan modificar el diseño orginal que Microsoft dio a su producto Windows. De hacerlo, atentaría contra el derecho de propiedad de la empresa.
- Y entonces, ¿cuál es la solución?.
- Microsoft tendría que revelar la función de esta segunda clave. Decir cuáles son las condiciones en que logró la licencia de exportación, hablar con los programadores que la pusieron allí y ver qué es lo que pasa. Hasta que eso no suceda, nadie sabrá con certeza qué sucede.
- ¿Cree que eso suceda?.
- No tengo la menor idea. Microsoft nunca explica lo que hace.
- ¿Cuáles serían las peores consecuencias de que no se hiciera nada por remediar la existencia de esta "puerta trasera" a Windows?.
- Tampoco lo sabemos. No se puede ignorar que estamos tratando con una agencia que se dedica al espionaje. Además, pienso que Microsoft ni siquiera está preocupada, porque la gente no tiene otra opción que comprar Windows.
- Pero están saliendo otros programas.
- Sí, está el Linux, que es bueno para centrales de datos, pero no para trabajo de escritorio ni para el usuario común. Microsoft es un monopolio y si no da ninguna respuesta clara frente al tema, jamás sabremos qué pasó.
- ¿En Cryptonym han descubierto casos como éste en el pasado?.
- Cuando hacemos audiencias de seguridad, encontramos debilidades, cosas que podrían ser utilizadas como puertas traseras de un sistema. Pero también hemos encontrado muchas estupideces. Quizás Microsoft esté diciendo la verdad y se trate de una clave de respaldo. Pero, de ser cierto, estarían reconociendo que fueron lo suficientemente estúpidos para hacerlo. Ahora, yo podría dar seis razones de por qué es una clave para la NSA y otras seis de por qué no lo es. Sin embargo, nada de lo que ha dicho Microsoft me ha convencido de que no lo sea.

Revista QuePasa 1484
Lunes 20 de setiembre 1999

Mentiras arriesgadas y sobre los gobiernos que se dejan seducir por ellas

http://seguridad.internautas.org/articulo.php?sid=282
http://www.rebelion.org/cibercensura/040214fa.htm

Domingo, 15 de Febrero de 2004
En septiembre de 1999 el criptógrafo Andrew Fernandes, http://www.fernandes.org/andrew.html mientras examinaba el código de un parche de seguridad de Windows, descubrió una etiqueta denominada NSAKEY y a partir de ese momento, la polémica estaba servida. Como consecuencia de esta noticia, aparecieron opiniones en todos los idiomas y defendiendo todas las posturas posibles, incluso calificando esta noticia como un "hoax" (mentira difundida por Internet).
http://www.quepasa.cl/revista/1484/38.html

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/news/backdoor.asp.
Sin esperar mucho, el día 3 de septiembre de 1999 la NSA (Agencia de Seguridad Nacional de EEUU) y Microsoft lanzaron un comunicado conjunto negando la noticia. Al día siguiente, Microsoft hizo unas declaraciones en el Washington Post indicando que la etiqueta se usaba para marcar que la clave en cuestión, cumplía con los estándares técnicos de la NSA y que no se trataba de una puerta trasera. Pero a muchas personas y gobiernos, como es lógico, este turbio asunto les pareció como poco inquietante.

Con independencia de la polémica, muchos técnicos y expertos en seguridad informática de todo el mundo, comenzaron a temer que realmente hubiera una alianza entre Microsoft y la NSA. De hecho, parece algo tentador y plausible, si tenemos en cuenta que dicho sistema operativo, o el conjunto de los productos de Microsoft, representan casi un monopolio y están presentes en más del 97% de los ordenadores de todo mundo. Para hacerlo más plausible aún, basta con revisar las referencias históricas relativas a los esfuerzos de los EEUU para conseguir información de inteligencia por todos los medios posibles. Como muestra podemos hacer referencia a la cara, compartida y sofisticada red Echelon, tan negada en su momento por los gobiernos participantes y en especial por los EEUU, cuando ahora sabemos que es algo muy real y tangible.
http://altavoz.nodo50.org/echelon2000.htm.

No cabe duda de que una puerta trasera en los productos de Microsoft es algo muy tentador para cualquier gobierno, si se puede controlar a voluntad. Su existencia representaría una forma económica, segura, eficaz y rápida de obtener cualquier tipo información de inteligencia procedente de cualquier parte del mundo. Incluso se podría pensar en la posibilidad de controlar remotamente sistemas informáticos y con ello, los equipos o las instalaciones asociadas, sin necesidad de moverse de casa. Recordemos también que las puertas traseras no están restringidas a los productos de Microsoft y la existencia de puertas traseras, con una u otra finalidad, ya han aparecido en algunas aplicaciones informáticas, por lo que ese inquietante hecho no se puede considerar como algo improbable.

Algunos gobiernos, conscientes del enorme riesgo que podría suponer la existencia de esas puertas traseras para los sistemas que contenían información sensible, decidieron tomar medidas urgentes sin necesidad de esperar a más confirmaciones ni debates. En la toma de decisiones, al margen de la posibilidad más o menos cierta de que existieran puertas traseras, también influye el hecho palpable de que productos de Microsoft presentan otros problemas de seguridad igualmente graves. Los virus o los troyanos, por ejemplo, son fuentes de muchos problemas y motivo frecuente de graves pérdidas económicas para los usuarios, lo que es un problema adicional en los sistemas críticos.
http://www.soportelinux.com/articulo.php?articulo_id=7.

Uno de los primeros países que dieron el paso para eliminar los productos de Microsoft de los sitios sensibles, fue Alemania. Este país de forma inteligente y en un tiempo récord, eligió GNU/Linux como una alternativa lógica, madura y segura a sus problemas de seguridad. Otros países, como China por ejemplo, mostraron su preocupación por la posibilidad de que se pudiera acceder a la información contenida en sus sistemas gubernamentales y posteriormente, tomaron medidas diversas. Pero lo más significativo y sorprendente, es que hasta los EEUU, conscientes de la posible inseguridad y de los problemas relacionados con los productos de Microsoft, decidieron usar sistemas de fuente abierta en sus sistemas sensibles y en especial, en los relacionados con la defensa nacional. No cabe duda de que eso lo hicieron al margen de la posibilidad de las puertas traseras, puesto que en teoría las controlaban ellos.

http://www.noticiasdot.com/publicaciones/2002/0602/0206/noticias0206/noticias0206-16.htm.

En un intento de eliminar esas dudas razonables y razonadas hasta la saciedad sobre la seguridad de sus productos y recuperar así, parte de su deteriorada imagen de seguridad, Microsoft, entre otras medidas, diseñó un proyecto de compartición de código que se denominó GSP (Government Security Program)
http://www.microsoft.com/presspass/features/2003/Jan03/01-14gspmundie.asp.

Según este proyecto, Microsoft permitiría, a los países interesados en ello, el acceso controlado y autentificado a aparte de su código fuente. Recientemente parte del código de Windows se ha filtrado y cuelga en Internet. Microsoft defiende la necesidad de no mostrar código para que nadie, que cuente con los conocimientos adecuados, pudiera atacarlo y explotar las vulnerabilidades que encontrara, cosa que es lógica puesto que el modelo de desarrollo de la empresa es cerrado y no colaborativo.

La compartición de este código se ha criticado duramente y en muchas ocasiones, por expertos de seguridad de todo el mundo y a la vista del desarrollo posterior de los hechos, hemos de pensar que esas críticas deberían haberse tenido en cuenta por más gobiernos. La iniciativa GSP sido considerada por lo expertos de dudosa eficacia, peligrosa y poco rentable para los gobiernos que la pudieran suscribir.
http://www.hispalinux.es/noticias/160
http://www.hispalinux.es/noticias/159
A cualquier experto en informática se le ocurren muchas técnicas para que la revisión del código fuente de un programa revele lo que no interesa. En este caso, es más sencillo puesto que se establecen limitaciones al acceso y no se controla todo el proceso de generación del código ejecutable, que incluye el código fuente de las librerías y compiladores, o a la posibilidad de generar, ejecutar y probar el programa de forma local. Aclaremos que la propuesta de Microsoft no tiene nada que ver con el software de fuentes abiertas, o con el software Libre, aunque Microsoft ha intentado vender algunas similitudes para mayor confusión de los usuarios.

Uno de los países que se prestó a la maniobra de Microsoft fue España http://iblnews.com/noticias/01/98285.html y el CNI (Centro Nacional de Inteligencia) ha obtenido acceso reciente al código fuente incompleto de los productos de Microsoft. Si tenemos en cuenta que en la administración española mantiene sistemas y programas de Microsoft desde la versión 95 a la versión XP, podemos pensar que el CNI tiene un trabajo de titanes puesto que cada versión tiene millones de líneas de código fuente. No cabe duda de que la responsabilidad asumida es grande. Si el CNI no es capaz de encontrar puertas traseras, o fallos de seguridad que pudieran ser explotados, o si los encuentra, no los publica y los usa en beneficio propio, estaría creando una falsa sensación de seguridad altamente peligrosa. Pero como veremos seguidamente, las puertas traseras aunque las haya en los ejecutables, no se encontrarán por el CNI, ni por nadie que acceda a código fuente de Microsoft.

Para desgracia de nuestro gobierno y el CNI, en el CiberPaís del 12 de Febrero de 2004 hay una esclarecedora entrevista a un eminente experto en seguridad informática, que ha trabajado en ocasiones para Microsoft. Se trata de Hugo Scolnik, una persona madura y de prestigio internacional, que es Doctor en matemáticas por la Universidad de Zurich (Suiza) y consultor de la Unesco. Scolnik que ha colaborado en la Ley de Firma Digital de Argentina, país en el que reside, también ha desarrollado proyectos de criptografía y seguridad, para los principales bancos de ese país. Esta persona sobre la que no cabe ninguna duda de su honestidad y que goza de prestigio internacional, ha contestado a algunas preguntas de la periodista del CiberPaís y entre ellas, hay dos muy significativas, que aclaran muchas dudas y que implican la toma de acciones inmediatas por los responsables de seguridad de muchos países y empresas.

Peridodista: ¿No son los Gobiernos quienes quieren controlar a los ciudadanos y conocer la clave de acceso al cifrado?
Scolnik: La política de EEUU durante mucho tiempo ha sido tratar de que no hubiera criptografía fuerte para las personas comunes. Discutimos muchísimo con autoridades de EEUU tanto por el proyecto que hicimos con Microsoft como con el FBI y otras agencias. Mi posición particular es que la gente peligrosa tiene acceso a la criptografía fuerte.
Peridista: ¿Tienen puerta trasera?
Scolnik: Nosotros hemos fabricados métodos que no pasan por el control de ningún Gobierno. Cuando trabajábamos con Microsoft, con cada cambio teníamos que enviar el código fuente a la NSA, donde lo compilan y agregan lo que quieren y luego vuelve como producto que nosotros distribuimos. No se que es lo que pusieron. En paralelo se han hecho muchos métodos sin puerta trasera, algo que es muy importante para asegurar la privacidad de las personas.

Estas afirmaciones son bastante claras, se corresponden a sospechas que ya se tenían y representan un motivo suficiente como para que se tomen medidas urgentes por parte de los particulares, empresas, gobiernos y administraciones que usan software de Microsoft.

Analicemos la situación. Está claro que el programa de GSP (Government Security Program) es una falacia, es inútil y representa una pérdida de tiempo y esfuerzos. Esfuerzos que se podrían dedicar a mejorar y adaptar los programas de fuentes abiertas a necesidades específicas de los gobiernos e instituciones. Los motivos son obvios:

1)El problema no está en el código fuente de Microsoft ni en el de ninguna de las aplicaciones que corren sobre los sistemas operativos de esta empresa, está en el ejecutable modificado por la NSA, que es lo que le llega al usuario. Esto implica que lejos de ver el código fuente, lo que hay que hacer es desensamblar el que se ejecuta, lo que no siempre es sencillo ni viable.

2)A la luz de las declaraciones de Scolnik, el ámbito de búsqueda se amplía a cualquiera de las aplicaciones que se ejecutan sobre los distintos sistemas operativos de Microsoft y no sirve de nada disponer del código fuente de Microsoft o sus socios tecnológicos para poder comprobarlo.

Esta es la maniobra perfecta de inteligencia, se permite el acceso a la criptografía fuerte por los usuarios y se crea un falso clima de seguridad. Cuando los sistemas tienen la información que se desea, se accede a ella, ya sea mediante puertas traseras, claves maestras, o explotado vulnerabilidades no publicadas. Por su fuera poco, este software además de los problemas e incertidumbres de seguridad que crea, por los costes asociados supone una enorme sangría económica para las empresas y las administraciones que lo usan, lo que contribuye, con cifras astronómicas, al desequilibrio de la balanza de pagos de muchos países con los EEUU, es el círculo perfecto. Es curioso que se intente conseguir el déficit cero, pero no se tomen en cuenta otras medidas para lograrlo.

Las conclusiones son muy claras. España no debería haber entrado en el peligroso juego de Microsoft. Esta empresa, aunque no ha mentido nunca, no ha contado toda la verdad sobre lo que se ejecuta en los ordenadores. Es cierto que su código fuente no tiene puertas traseras y que está intentando mejorar la seguridad de sus programas, pero de lo demás no dice nada y lo que no nos creemos, nos cuesta mucho probarlo. El Centro Nacional de Inteligencia no debería hacerle el juego a una empresa privada extranjera, colaborar con ellos en la mejora de la seguridad de sus productos y al mismo tiempo, crear falsas expectativas de seguridad en los ciudadanos, en la administración, o en las empresas.

No entraremos en el análisis del cuerpo legal aplicable en este caso, que está bastante claro y es prolijo en lo que respecta a la protección de la información y la intimidad de los ciudadanos. Por el momento, nos basta con recordar un artículo de nuestra Carta Magna:

Artículo 18

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

No cabe ninguna duda en la interpretación de este claro artículo y es deseable que los responsables gubernamentales tomen conciencia de estos problemas y sean capaces de tomar las medidas adecuadas de forma que el artículo 18 de la Constitución Española se cumpla en toda su dimensión. No se pueden anteponer los derechos básicos de los ciudadanos, a los intereses de una empresa extranjera, o las maquinaciones de otros gobiernos, aunque sean amigos. Si no se hace así, se pueden derivar consecuencias negativas para la Seguridad Nacional, para los intereses económicos de la nación y evidentemente, no se garantizarán las libertades fundamentales de los ciudadanos contenidas en la Constitución.

Afortunadamente hay una alternativa, segura, rápida, eficaz y económica a este y otros muchos problemas relacionados con el software. Se trata de una alternativa altamente recomendada y debatida en foros de reconocido prestigio internacional. La solución se llama Software Libre, o Software de Fuentes Abiertas, que es posible que acabe declarándose como Patrimonio de la Humanidad. Este es software que no está controlado por ninguna empresa o gobierno, permite un control absoluto de lo que se está ejecutando en un ordenador y permite corregir, si fuera necesario, cualquier fallo de seguridad que se pudiera presentar. Por sus virtudes, el Software Libre se está usando con un gran éxito en muchos sitios y todas las experiencias indican que es deseable su uso a todos los niveles y en especial, en las aplicaciones en las que las necesidades de seguridad son máximas.

Puede que no sea necesario ni aconsejable recurrir a la confirmación de que existan o no puertas traseras en el software de Microsoft, la simple sospecha de ello debería bastar para tomar las medidas adecuadas, como le bastó a Alemania en su momento. Que no se pueda demostrar la existencia de puertas traseras, o que no se puedan encontrar, puede que no sean motivos suficientes para no tener en cuenta tal posibilidad. Por si fuera poco, todos los indicadores, incluidos los económicos y los sociales, marcan que el Software Libre es el camino a seguir y así se está asumiendo en muchos sitios.

Hemos de ir pensando en instalar Software de Fuentes Abiertas en todos nuestros sistemas de la Administración y en especial, los relacionados con la Seguridad Nacional, si queremos estar seguros de que nadie accede a nuestros datos y que las garantías constitucionales están garantizadas. Del mismo modo, el Ministerio de Ciencia y Tecnología debería tomar conciencia de este asunto y sus consecuencias negativas, e iniciar campañas institucionales recomendando a los particulares y las empresas, la necesidad de mejorar su seguridad. Puede la mejor forma de hacerlo sea recomendando y fomentando el uso de Software Libre.

Fernando Acero (Febrero 2004)
Se permite reproducir y distribuir este artículo sin modificar e indicando el autor del mismo.
- --
Fernando Acero Martín
Una oportunidad para todos en http://gestion-libre.hispalinux.es

---

Microsoft permite que el Gobierno de EEUU espíe los PC

http://www.el-mundo.es/navegante/99/septiembre/05/microsoft.html

US secret agents work at Microsoft: French intelligence

http://www.politrix.org/foia/nsa/nsa-ms-spy.htm

Microsoft's Backdoor for "NSA" Spys

http://www.geocities.com/~budallen/backdoor.html

Bill Gates: un agent des services secrets américains ?

http://solutions.journaldunet.com/99sept/990907nsakey.shtml

Crypto expert: Microsoft products leave door open to NSA

http://www.cnn.com/TECH/computing/9909/03/windows.nsa/

Saludos.
Kbza Kbza37@yahoo.com
