>> Jorge Dávila

La seguridad de Internet como objetivo

Con más de diez meses de retraso, la administración norteamericana convocó a finales de 2003 una primera reunión para llamar la atención del sector industrial de las TIs sobre la asignatura pendiente que supone la iniciativa del Presidente Bush para hacer más seguro el ciberespacio. El nuevo mensaje de la administración parece más firme que el anterior, pero la respuesta empresarial no parece haber sido la movilización general. Las ideas que se han presentado en esa reunión no son nuevas, pero su análisis nos puede dar una idea de sí podemos esperar algún resultado real de la cruzada americana para hacer segura Internet.

El pasado 3 de diciembre de 2003 se celebró en Santa Clara, California, una reunión[1] sobre seguridad en Internet. Este encuentro fue convocado por la División de Seguridad Nacional del recién creado Departamento de Seguridad Interior (DHS). Como ya mencionamos en números anteriores de SIC, este departamento nació a raíz de la iniciativa del Presidente Bush, "*Strategy to Secure Cyberspace*[2]", que fue publicada en febrero de 2003 y que debemos ver como uno de los efectos colaterales del 11 de septiembre de 2001.

Entre los participantes de esa reunión estaban Tom Ridge como secretario del DHS y su asesor en los temas de protección de la infraestructura, Bob Liscouski. También participó Amit Yoran como nuevo director de la National Cyber Security Division. Esta reunión también fue patrocinada por varias asociaciones empresariales norteamericanas como son la Cámara de Comercio, la Business Software Alliance, la Information Technology Association of America, y TechNet.

Un hecho a tener muy en cuenta es que en la reunión del 3 de diciembre un importante grupo de desarrolladores de software parecen haberse caído de la lista de invitados: Red Hat, SuSE y otras compañías Linux no estaban representadas en los grupos de trabajo de Santa Clara.

En esta reunión los responsables del sector público y algunos del sector privado pusieron en común sus opiniones sobre cómo la National Cyber Security Division podría intentar hacer realidad la ambiciosa iniciativa presidencial. Hay que llamar la atención sobre el hecho de que este ha sido el primer foro público que se ha celebrado desde la publicación de la iniciativa de la administración Bush en febrero de 2003.

Los objetivos de la reunión eran conocer las opiniones, puntos de vista y, por qué no, establecer compromisos de los líderes de los sectores público y privado, sobre qué prioridades e hitos pueden apoyar a la National Cyber Security Division, en su cometido de mejorar la seguridad en Internet y fortalecer la capacidad de los EEUU en la prevención y respuesta ante los ciber-ataques terroristas sólo por ellos vaticinados.

Para conseguir estos objetivos, la reunión se organizó en cinco grupos, cada uno de ellos afrontando alguno de los retos clave identificados en la estrategia de G. Bush: **[1]** Sensibilización de los usuarios domésticos y de las pymes; **[2]** Los sistemas de advertencia temprana en temas de ciber-seguridad; **[3]** El funcionamiento de las empresas; **[4]** Los estándares técnicos y criterios comunes, y **[5]** La seguridad a lo largo del ciclo de desarrollo del software. Estos cinco grupos serán los responsables, en los próximos meses, de desarrollar recomendaciones y planes de trabajo específicos que las hagan realidad el plan director original.

> ***La idea de que se pueda hacer una herramienta que detecte y corrija los fallos que los programadores humanos no han sido capaces de detectar, es una quimera; la seguridad es un concepto que va más allá de las líneas que se ejecutan en un procesador y todavía está lejos de ser algo realizable en exclusiva por autómatas.***

Estos grupos de trabajo se han comprometido a emitir sus conclusiones antes del 1 de marzo de 2004 y en ellos harán públicas sus recomendaciones para, entre otras cosas, la creación de un software más seguro. La siguiente reunión de los grupos esta fijada, en principio, para septiembre próximo, fecha límite para que cada grupo publique, al menos, algún resultado.

Además de las buenas palabras habituales en estos actos, en esta reunión los representantes del gobierno federal americano advirtieron a los líderes de la industria de la seguridad en Internet que si no se encargaban ellos, por iniciativa propia, de liderar la "securización" del ciber-espacio, entonces tendrían que terminar haciéndolo sometidos al cumplimiento de futuros requisitos legislativos.

De hecho, hay algo de lógica en esta advertencia ya que en EEUU el sector privado es, como no podía ser de otro modo, responsable del 85% de la infraestructura crítica del país y, en consecuencia, es un personaje esencial a la hora de implementar cualquier plan nacional sobre ciber-seguridad, sea el del presidente Bush o de cualquier otro. Por analogía con otros ámbitos de la vida norteamericana reciente, el argumento utilizado para urgir este bastionado informático es el de aceptar, como acto de fe, que los terroristas están buscando ya el modo de atacar dichas infraestructuras. La realidad del ciber-terrorismo es algo bastante cuestionado en otro foros pero en la América de Bush gusta poco hacer poner en duda las afirmaciones de la Casa Blanca y uno llega a sentirse intimidado en el día a día si osa dudar de la posición oficial.

Robert Liscouski, asesor del secretario del DHS para la protección de la infraestructura, pidió al sector privado algo más que una promesa de trabajar juntos y formar grupos de trabajo; solicitó que se establecieran métricas y documentos abiertos que mostrasen los resultados obtenidos, en vistas a que el DHS puedan preparar las iniciativas legislativas pertinentes. Dicho de otro modo, *el gobierno de los EEUU pide ideas, soluciones para defenderse de las amenazas identificadas y poder convertirlas en leyes federales.*

La respuesta del sector empresarial americano no ha parecido ser suficiente y de ahí la convocatoria de la reunión en Santa Clara. Donde sí se ha movido activamente el sector industrial, como por ejemplo la Information Technology Association of America y la BSA, es para presionar ante el gobierno federal y evitar cualquier propuesta normativa que les hiciese publicar o compartir datos relativos a sus regulaciones internas en temas de seguridad.

Ron Moritz, vicepresidente de eTrust Security Solutions de Computer Associates y co-director del grupo de trabajo *Security Across the Software Development Life Cycle* dijo que espera que la reunión del 3 de diciembre dé como resultado planes de acción concretos: «*A la industria le gustaría decir que nos reunimos dos días y ya tenemos todas las respuestas, pero mucho de esto va para largo*», comentario que no manifiesta demasiada confianza en el éxito de esta reunión.

Una visión más crítica de este evento interpreta que la celebración de esta reunión ha sido, simplemente, el primer acto público de Amit Yoran[3] como director de la National Cyber Security Division. Yoran se incorporó a su nuevo puesto en octubre pasado después de una larga y lenta búsqueda en la que algunos de los nombres más conocidos de la industria de la seguridad americana declinaron aceptar dicho puesto.

La propuesta del presidente Bush fue criticada desde el principio por tratarse de una iniciativa "voluntaria" y se llegó a decir de ella que "*no tenía dientes*", ya que no contenía medidas disuasorias concretas por lo que se quedaba en un "*bonito comunicado de prensa*". En principio, la administración de Bush declaró que no trataría de regular la industria de la seguridad en Internet, pero sí presionaría a las compañías para que proporcionasen un mejor software. El modo de hacerlo sería contratando sólo con aquellas empresas que satisfagan sus planteamientos básicos en aspectos tan variopintos como: tener implementada la autenticación en sus redes, disponer de una configuración gestionada de sus sistemas, proceder al entrenamiento de sus empleados en prácticas de seguri-

[1] http://www.us-cert.gov/events/summit
[2] http://www.whitehouse.gov/pcipb/cyberstrategy-draft.pdf
[3] Amit Yoran tiene experiencia en la industria de la seguridad y su empleo anterior era el de vicepresidente para la Gestión de Servicios de Seguridad de Symantec.

dad, establecer equipos para la resolución rápida de incidencias, tener organizados equipos de gestión de la seguridad, analizar periódicamente sus redes y utilizar procedimientos para asegurar que sus productos finales tienen una seguridad "suficiente".

Lo curioso es que la iniciativa de la administración Bush se parece bastante a la del presidente Clinton[4], «*A Framework for Global Electronic Commerce*», en eso de que sea la propia industria la que lidere el cambio hacia una Internet segura, por lo que este nuevo intento no supone un cambio sustantivo en el enfoque de la administración americana respecto a la seguridad digital. Si en la era Clinton este procedimiento "voluntario" no funcionó, no hay nuevas razones para esperar que lo haga ahora. La única diferencia significativa que hay entre ambos intentos de hacer segura Internet es que, en el documento de Clinton la seguridad informática era sólo un capítulo, y en el de Bush es todo el documento. Quizás esto sea un avance.

Lo que está claro para todo el mundo (capitalista) es que las compañías no cambiarán ni en un ápice su comportamiento y calidades actuales hasta que les fuerce a ello la presión del mercado o les obliguen las administraciones a través de nuevas y más "persuasivas" leyes que se hagan cumplir. Mientras en EEUU las propuestas sean de carácter voluntario, sin duda no va a cambiar nada o los cambios serán muy lentos. Lo que es un hecho es que el gobierno norteamericano publicó el plan Bush de ciber-seguridad hace casi un año y se ha hecho muy poco para poner en marcha las docenas de recomendaciones y sugerencias contenidas en dicho documento.

Control del desarrollo de software

De todos los temas tratados en la reunión de Santa Clara, me gustaría resaltar que el grupo de trabajo encargado del ciclo de desarrollo del software se centró en la posibilidad de ampliar las **especificaciones técnicas** y los **programas gubernamentales** para la **evaluación de la seguridad** y así poder aplicarlas a más productos de la TIs. Esa comisión plantea que los desarrolladores de software tengan que utilizar "nuevas herramientas" para detectar y eliminar automáticamente vulnerabilidades conocidas durante el desarrollo del software, y así alcanzar ciertos niveles mínimos de certificación.

El problema es que esas herramientas o no existen, o son muy poco eficientes o resultan caras por lo que todavía es necesario un esfuerzo importante para crear (si es que pueden llegar a existir) esas herramientas certificadoras que eliminen los fallos de seguridad nacidos de la ignorancia de los diseñadores/desarrolladores o de errores fortuitos.

La idea de que se pueda hacer una herramienta que detecte y corrija los fallos que los programadores humanos no han sido capaces de detectar, es una quimera que no tiene nada de nueva. El deseo de disponer de entornos de programación que simplifiquen lo más posible los esfuerzos del programador es algo que justifica todo el trabajo hecho en lenguajes y compiladores desde que la misma informática existe. La seguridad es un concepto que va mas allá de las líneas que se ejecutan en un procesador y todavía está lejos de ser algo realizable en exclusiva por autómatas.

Otra planteamiento más realista es que se haga un esfuerzo por establecer las reglas, procedimientos y protocolos de ensayo y evaluación, etc., que permitan ayudar a detectar y erradicar ciertos errores "gordos" en el desarrollo del software. Si se dispusiese de esas normas o procedimientos, lo natural sería convertirlas en necesarios desde un punto de vista legal. Esta solución no es cosa distinta en nada a cualquier otro proceso de "normalización de productos" bajo los criterios de una administración soberana.

Determinar la seguridad de Internet

La posibilidad de mejorar la seguridad en los sistemas de información y en las redes de comunicaciones está limitada superiormente, por ejemplo, por la seguridad de los sistemas operativos sobre los que se ejecutan el resto de aplicaciones. Por ello, la seguridad de los sistemas operativos y su **correcta configuración** son temas de vital importancia para determinar la seguridad de Internet.

Por no mencionar numerosas y vetustas iniciativas anteriores, digamos que el Institute of Electrical and Electronics Engineers (IEEE) ha empezado muy recientemente a trabajar en otro nuevo estándar que formule un umbral mínimo para los requisitos de seguridad que deben satisfacer los sistemas operativos de propósito general que corren en la inmensa mayoría de ordenadores en Internet. El estándar, IEEE P2200, «*Base Operating System Security*" (BOSS[5]), pretende afrontar tanto las amenazas externas como los fallos inherentes al diseño del software y a la práctica ingeniería en general. Los promotores de esta iniciativa piensan tener el estándar completo al final de 2004.

El objetivo de hacer una Internet segura pasa por definir qué se entiende por seguridad en cada caso y esa es la tarea más difícil de todas. Al ser Internet un organismo vivo carente de patrón, ira evolucionando con el tiempo y en esa evolución definirá lo que ella entiende por seguridad.

Esta iniciativa se ha constituido bajo la guía del National Institute of Standards and Technology (NIST) americano en términos de los "*Protection Profiles*" propios de la ISO en su iniciativa conocida como Criterios Comunes ("*Common Criteria*"-CC). Este estándar tratará las funciones esenciales para aportar seguridad entre plataformas distintas, e incluirá la identificación, la autenticación y el control de accesos, entre otros temas.

El estándar tendrá un cierto número de limitaciones, ya reconocidas por sus promotores, puesto que un mismo estándar no puede ser compatible con las peculiaridades de todos los sistemas operativos. Además, el uso estricto de los *Common Criteria* de ISO es opcional, y el estándar final puede terminar no pareciéndose al documento inicial propuesto por el NIST. Este estándar de consenso persigue armonizar las aportaciones de todos los agentes involucrados, incluyendo a los desarrolladores de sistemas operativos, al mundo académico y a los usuarios de la administración, del sector financiero, del control de procesos y otros.

Gary Stoneburner, vicepresidente del BOSS Working Group, resalta que este estándar regresará a las bases de la "**Information Assurance**" y a la necesidad de tener expectativas razonables y claras respecto a lo que se entiende por seguridad mínima de los futuros sistemas operativos. La aparición de esta iniciativa en estas fechas no es casual, y pretende transformar el edicto de la administración Bush en un consenso comunitario.

El grupo de trabajo BOSS surge dentro de una nueva comunidad dentro de IEEE que pretende hacer realidad todo el potencial de las TIs para proporcionar la información que genera, distribuye y almacena. Las actividades de esta comunidad incluyen otros estándares interesantes como son el IEEE P1618, "*Public Key Infrastructure Certificate Issuing and Management Components*» y el IEEE P1619, *Architecture for Encrypted Shared Media*[6]. Sus promotores esperan poder tener listo el nuevo estándar en un año e invita a los expertos en ingeniería del software o métricas, ciberseguridad, desarrollo de sistemas operativos o áreas relacionadas, a participar activamente en esta iniciativa.

A la vista de todo lo anterior, da la impresión de que la iniciativa del presidente Bush va con cierto retraso y que "El Dorado" de hacer segura La Red, según los criterios de la administración norteamericana, es algo que está muy lejos de ser posible. Una de las posibles causas de la lentitud de esta historia quizá esté en el poco peso específico real que tiene la administración pública en la sociedad americana, y en que los criterios de seguridad expuestos a principios de 2003 siguen siendo ajenos a los criterios comerciales actuales. Las amenazas veladas del nuevo Departamento de Seguridad Interior (DHS) de los EEUU son poco coercitivas y nada nuevas, y parecen más estar hechas "cara a la galería" que ser un giro significativo en los modos de operar de la sociedad americana en Internet.

El objetivo de hacer una Internet segura pasa por definir qué se entiende por seguridad en cada caso y esa es la tarea más difícil de todas. Al ser Internet un organismo vivo carente de patrón, ira evolucionando con el tiempo y en esa evolución definirá lo que ella entiende por seguridad. Desde el punto de vista técnico, los problemas correctamente planteados van siendo resueltos, y los que se resisten, probablemente tienen un enunciado inicial mal planteado. ■

Jorge Dávila Muro
Director
Laboratorio de Criptografía
LSSI - Facultad de Informática - UPM
jdavila@fi.upm.es

[4] http://www.technology.gov/digeconomy/framewrk.htm
[5] http://bosswg.org/
[6] Para obtener mas información, ver: http://ieeeia.org/