



Horizontes definidos y ¿lejanos?

El informe trata temas que involucran directamente a las organizaciones europeas de normalización y llama a éstas y a sus homólogas empresariales para que se pongan finalmente de acuerdo, y mejoren la situación actual en cuanto a la disponibilidad de comunicaciones electrónicas seguras; en particular en lo que se refiere al comercio-e y al intercambio de información, tanto en el seno de la UE, como con terceros países.

Las acciones básicas mencionadas en el llamamiento de la Comisión son:

– Acelerar los trabajos de las organizaciones europeas de estandarización que tengan que ver con la interoperabilidad de productos y servicios seguros, y que ello se haga dentro de un calendario ambicioso.

– La Comisión reitera el uso de las firmas electrónicas, el desarrollo de PKIs de operación sencilla y fácil uso, así como continuar con el desarrollo de los sistemas IPv6 e IPSec.

– La Comisión invita a promover el uso de procedimientos de certificación y acreditación a través de estándares europeos e internacionales, y que se favorezca el reconocimiento mutuo de certificaciones.

– La Comisión llama a los agentes del mercado europeo a participar activamente en las actividades de estandarización europeas e internacionales.

Todo esto ocurre a la vista de que, según el informe del European IT Observatory para 2003, el análisis del mercado europeo pone de manifiesto que los gastos del usuario final en temas de seguridad supusieron un total de **9,4 billones** de euros en 2002; y que esa cifra se aproximará a los **12 billones** de euros en 2003, y a **18 billones** en el 2005.

Para la Comisión, los incidentes de seguridad se pueden agrupar en las siguientes categorías:

– Las comunicaciones electrónicas pueden ser interceptadas y los datos copiados o modificados, dañando la intimidad de los individuos y facilitando la explotación ilegal de esos datos.

– El acceso no autorizado a ordenadores y redes para la copia, modificación o destrucción maliciosa de datos, y que esto puede extenderse a los sistemas domésticos empotrados.

– Los ataques disruptivos en Internet y, en el futuro, en las redes de telefonía que se harán más y más vulnerables.

– El software malicioso que puede “tumbar” los ordenadores, eliminar o

La respuesta de CEN¹ y ETSI² a la comunicación de la Comisión Europea sobre una política europea de seguridad ya está disponible para su escrutinio público. Este informe-titulado “Network and Information Security: Proposal for a European Policy Approach”- pretende ser una respuesta para desarrollar una estrategia global, clara y concreta sobre la seguridad en redes electrónicas. Este informe y la comunicación de la Comisión tratan temas de normalización y tocan a arrebato para que todo el mundo se ponga finalmente de acuerdo y mejore la situación actual en cuanto a comunicaciones electrónicas seguras.

modificar datos o reprogramar los equipos domésticos automáticos.

– La suplantación de usuarios y entidades puede causar daños sustanciales (entrada de software malicioso, los contratos podrán ser repudiados, desvelado de informaciones confidenciales, etc.)

Para la Comisión sigue estando claro que proporcionar una infraestructura confiable y segura sobre la que realizar comunicaciones electrónicas en el “cyberspace” animará el crecimiento del *e-business* en Europa. Para ello todos los personajes de ese escenario deben aceptar la responsabilidad de tomar las medidas a su alcance para asegurar globalmente el sistema, y luego convencer a los usuarios de que hacer negocios de ese modo no sólo es eficiente, sino también seguro. El *e-business* la Comisión lo entiende como la realización de una transacción comercial normal pero sobre una red electrónica; no obstante, hay otras actividades no mercantiles que requieren niveles de seguridad similares o superiores. Un buen ejemplo de ello es la “Sanidad digital” (“*e-health*”), donde la seguridad de las comunicaciones es mucho más necesaria, ya que está ahí para proteger la intimidad básica de los pacientes.

La respuesta de CEN y ETSI se centra en el uso seguro de redes IP genéricas pero hace referencia explícita a las redes virtuales privadas, LANs inalámbricas y redes móviles 3G, ya que es probable que muchas transacciones del esperado comercio electrónico terminen utilizando todos esos tipos de redes. Los autores de este borrador reconocen que hay pocas infraestructuras que garanticen la interoperabilidad real de los actuales sistemas, y también reconocen la ausencia de certificaciones apropiadas en algunas áreas del sector. El resultado de todo ello es la fragmentación actual y el improbable establecimiento de redes globalmente seguras a pesar de que sus partes sí puedan serlo. Para el CEN y el ETSI los puntos clave del futuro éxito serían favorecer:

– La **interoperabilidad**. Hay muchos estándares de seguridad distintos y eso lleva crear problemas de interoperabilidad. La evaluación de la interoperabilidad debe ser parte del proceso de estandarización.

– El **grado de actualización**. Dado que la seguridad no es un problema estático, las implementaciones de un estándar deben ser actualizadas cada vez que se detecta una debilidad, y los nuevos estándares deben eliminar el uso de los anteriores; los cambios de estándar debe hacerse de manera simple, transparente y documentada para que el usuario final pueda actualizar sus sistemas.

– El **tratamiento de los usuarios domésticos y las pyme**. En el futuro próximo estos colectivos tendrán conexiones permanentes a Internet como parte de sus actividades. Estos usuarios no tendrán ni experiencia ni inclinaciones propias a aplicar oscuras medidas de protección que eviten los quiebros de la seguridad de sus equipos.

El informe hace algunas recomendaciones para paliar los efectos de esta situación antes de que se convierta en un problema serio, pero menciona explícitamente que los usuarios de los equipos no se pueden escapar a la responsabilidad de la correcta instalación de sus equipos. Los fabricantes deben asumir la responsabilidad de proporcionar los instrumentos necesarios para hacer seguros los equipos que venden, pero no pueden asumir la responsabilidad de su correcto uso final. Así pues, según este informe, los usuarios deben aceptar las responsabilidades de que sus equipos, conectados a una red pública compartida, no dañen o incomoden a los demás usuarios.

El Informe del CEN y ETSI hace especial hincapié en los usuarios domésticos, y los agrupa en tres vertientes distintas: *Home-working*, *Personal Business* y el *Control Automático de Equipos Domésticos*:

Para terminar con la descripción de este informe, conviene destacar los servicios de seguridad en los que recomiendo prestar mucha atención:

1. Los *Servicios de Registro y Autenticación*, ya que son los responsables de identificar y dar acceso a los usuarios legítimos.

2. Los *Servicios de Confidencialidad y Privacidad*, ya que son los responsables de que la información intercambiada sea transferida y almacenada de forma segura.

3. Los *Servicios de Confianza*, que son necesarios para hacer trazables las transacciones de comercio-e entre individuos autenticados, de modo que no puedan ser rechazadas.

4. Los *Servicios de Negocio*, que aseguran y certifican que las aplicaciones de comercio-e usadas han sido diseñadas, configuradas y se operan de modo seguro, y que está al abrigo de ataques maliciosos y fallos accidentales.

5. Los *Servicios Defensivos* en redes, como conjunto de medidas para proteger los datos, tanto en tránsito como almacenados.

6. La Certificación de Servicios es lo que justifica la confianza del usuario en que las medidas técnicas y no técnicas son suficientes para protegerle de los riesgos asociados con el servicio. El resultado final es una “certificación” del servicio.

Estas son las características generales del informe del CEN y ETSI, y hay que resaltar positivamente que incluye una lista muy actualizada de las fronteras y los retos que hoy tiene la seguridad informática; lo que ya no es tan positivo es que si bajamos a la letra pequeña de sus recomendaciones nos encontraremos con frases mas o menos bonitas y todas ellas bastante obvias, por lo que esta respuesta no podemos considerarla demasiado “concreta”. A pesar de ello, es bueno que el panorama se aclare y que, al menos, sepamos cada día mejor a qué nos enfrentamos. Para mi, todavía hemos de esperar a que la iniciativa privada y empresarial realmente se moje en todo esto de hacer el ciber-espacio seguro y rentable. Estamos en un sistema económico en el que se le otorga a las empresas privadas los primeros personajes de este teatro por lo que, si ellas no se ponen en marcha, poco se podrá hacer y esperar. ■

JORGE DÁVILA MUÑOZ
Director
Laboratorio de Criptografía
LSSI - Facultad de Informática - UPM
jdavila@fi.upm.es

¹ CEN = Comité Europeo de Normalización (www.cenorm.be)

² ETSI = European Telecommunications Standards Institute (www.etsi.org/home.htm)