

La cooperación entre AAPP y sector privado, clave para mejorar la seguridad de organizaciones y ciudadanos



Hector Sánchez Montenegro
Chief Security Advisor.
Microsoft Ibérica

La seguridad informática se ha convertido en un tema de permanente actualidad. No falta en ningún foro, está presente en todos los debates, parece incluso que hay cierta expectación en la industria por saber cuál será la próxima vulnerabilidad, la hazaña que hará famoso al próximo hacker.

Y si se ha convertido en un contenido recurrente en la agenda de los medios ha sido por muchos motivos, pero especialmente por las consecuencias dramáticas que puede ocasionar a cualquier usuario, empresa o administración pública ser vulnerable o, simplemente, no tomar conciencia de la importancia que tiene la seguridad.

La seguridad informática es noticia casi todos los días por ser, también, uno de los sectores más activos de las Tecnologías de la Información. Las amenazas se multiplican a un ritmo vertiginoso. Los virus, gusanos, troyanos y demás son palabras que empiezan incluso a ser conocidas fuera del contexto de las TI.

Las tecnologías desarrolladas para combatir esos peligros se renuevan al mismo ritmo y hacen de la seguridad un área en constante evolución. Por eso es uno de los factores más sensibles a la hora de poner en marcha cualquier proyecto tecnológico. Internet se ha convertido en una herramienta

poderosa, pero también ha planteado nuevos problemas relacionados con ataques a cuestiones tan fundamentales como son la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas.

Por todo esto la seguridad se ha convertido en una de nuestras principales preocupaciones y en uno de nuestros compromisos más firmes.

Trabajamos para ayudar a solucionar estos problemas y queremos que el ciudadano tenga la misma confianza al realizar una compra electrónica que al realizar un pago en una tienda. Y por eso dedicamos casi un tercio de nuestra inversión en I+D, que aproximadamente es de 7.000 millones de dólares, a mejorar la seguridad informática. Un esfuerzo que compartimos con

“Internet ha planteado nuevos problemas relacionados con ataques a cuestiones tan fundamentales como son la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas”



las Administraciones Públicas que, en países como el nuestro, han hecho de esta cuestión una prioridad.

Las AAPP tienen necesidades especiales en el terreno de la seguridad informática y, a la vez, deben velar por la seguridad de los ciudadanos. En muchas ocasiones cuentan con responsables de seguridad y sus necesidades son similares a las de las grandes corporaciones. Porque compartimos sus preocupaciones y sabemos acercarnos a la complejidad de su infraestructura hemos establecido colaboraciones a largo plazo con el Gobierno español, compartiendo esfuerzos e información por incrementar el nivel de seguridad informática en nuestro país y proporcionar a todos los usuarios una experiencia informática segura, privada y fiable.

Las administraciones españolas, a la vanguardia en relaciones gobierno-ciudadano

Las AAPP españolas son, además, un modelo referenciado inter-

nacionalmente como buen hacer de relación telemática entre gobiernos y ciudadanos (nuestra Agencia Tributaria es un buen ejemplo de ello). Y en algunas ocasiones son las mismas Administraciones las que lideran determinados aspectos de la seguridad (DNI digital). Algunas administraciones centrales manifiestan incluso una especial responsabilidad de cara al ciudadano y han articulado organismos dedicados a resolver cuestiones relacionadas con esta materia como pueden ser Red.es, el Centro Alerta Antivirus o el recién estrenado Instituto Nacional de tecnologías de la Comunicación (INTECO).

Precisamente, con INTECO se firmó un acuerdo de colaboración orientado a fomentar la seguridad de los sistemas y las redes de información. El objetivo es crear un marco permanente para el desarrollo de iniciativas comunes y el

intercambio de información sobre potenciales situaciones de emergencia, asuntos comunes relacionados con virus y ataques informáticos que afecten a los ciudadanos o procesos de respuesta ante posibles amenazas e incidentes relacionados con la seguridad de redes y ordenadores.

Este acuerdo revela el interés de las AAPP por la seguridad, ya que forma parte del compromiso del gobierno por impulsar acciones dirigidas a salvaguardar la invulnerabilidad y privacidad de los sistemas y redes de información y, al mismo tiempo, colaborar con la iniciativa privada en la mejora de los niveles de seguridad en las aplicaciones utilizadas por ciudadanos y empresas.

El código fuente en manos del Gobierno

Pero este acuerdo no es el único que se ha firmado con el gobierno español. En diciembre del pasado año reforzamos nuestra relación con el Centro Nacional de Inteligencia (CNI) con la firma de un contrato que les permite acceder al código fuente de nuestro paquete ofimático Office. Gracias a esta alianza, los expertos en seguridad del CNI, que depende del Ministerio de Defensa, pueden acceder a la información técnica que precisen para auditar las características de dicho software, con el objetivo de mejorar la seguridad de los siste-

.....
“Las AAPP tienen necesidades especiales en el terreno de la seguridad informática y, a la vez, deben velar por la seguridad de los ciudadanos”

mas informáticos de la Administración.

Pero nuestra relación con el CNI es más antigua, ya que en enero del 2004 firmaron su adhesión al programa Government Security Program (GSP) que les dio acceso entonces al código fuente del sistema operativo Windows. El GSP fue puesto en marcha por Microsoft en 2003 para proporcionar a gobiernos e instituciones gubernamentales el acceso al código fuente de los principales productos de software de la compañía. El programa está diseñado para cumplir con las elevadas exigencias de seguridad de las administraciones de todo el mundo (se han acogido a él los gobiernos de Reino Unido, Noruega, Rusia, Australia, Países Bajos, Polonia o Grecia e instituciones como la OTAN) y proporciona la posibilidad de auditar el código fuente de Windows y Office mediante una herramienta de revisión específica. Mientras, desde Microsoft adoptamos el conocimiento de los expertos de entidades tan reconocidas como el CNI para conseguir, de manera conjunta, el desarrollo continuo de tecnología totalmente segura y fiable.

Juntos contra la pornografía infantil

También colaboramos con la Administración para promover y reforzar leyes destinadas a luchar contra el bombardeo *spam*, el *phishing*, que el año pasado costó a la banca española más de 50 millones de euros y que será una de las principales amenazas de 2007, o el abuso online de menores. Según la INTERPOL, el 50 por ciento de los delitos cometidos en la red están relacionados con la distribución,

difusión y venta de pornografía infantil y, según datos del FBI, desde 1996 el número de imágenes que contienen abusos a niños se ha incrementado en un 2.000%; sin embargo, las policías de todo el mundo sólo han identificado menos de 500 niños de los 50.000 (sólo el 1%) que se estima que han sido objeto de este tipo de abusos.

Para combatir esta situación, en octubre del año pasado Microsoft firmó un acuerdo con el Ministerio del Interior y la Fundación Alfonso Martín Escudero para aunar esfuerzos contra la pornografía infantil, un asunto para el que el presidente de la compañía, Steve Ballmer, se desplazó a nuestro país. El convenio permitirá al Cuerpo Nacional de Policía y a la Guardia Civil acceder a un programa de análisis e intercambio de información entre los cuerpos de seguridad de distintos países (CETS, Child Exploitation Tracking System).



Una herramienta de la que se beneficiarán nuestros cuerpos de seguridad, que ya se encuentran a la vanguardia de la lucha mundial contra esta forma de delincuencia. Los últimos datos sobre su actuación son de 2005 y dicen que se investigaron 203 casos de pornografía de menores a través de Internet y se detuvieron a 248 personas



relacionadas con ellos. De enero a agosto del año pasado se investigaron 187 casos y se detuvieron a 168 personas.

Con la plataforma de software CETS, en la que Microsoft ha invertido más de cinco millones de dólares hasta la fecha, se mejorarán los ratios de eficacia y cooperación policial en la persecución de los delitos relacionados con la pornografía infantil. El gran valor de la plataforma es la posibilidad de compartir toda esa información con organismos oficiales de otros países utilizando un "idioma informático" estándar, más allá del hardware o el software que utilicen en sus investigaciones. CETS facilita el almacenamiento, búsqueda y análisis de grandes cantidades de datos policiales, tanto en la fase de detección de los delitos como a través de todo el proceso de investigación, detención e inculpación. Ello permite conocer si un determinado asunto ha sido o está siendo investigado por otras unidades policiales del mundo.

La plataforma se implementó por primera vez en Canadá en el año 2003. El país cuenta hoy con cerca de 175 usuarios y sus fuerzas de seguridad están conectadas en nueve provincias. También se ha desplegado en Indonesia y actualmente se está implementando en varios países de Europa, entre ellos Italia y España. ◆