ieee.es
Instituto Español de Estudios Estratégicos

Documento
Análisis

20/2016 23 de marzo de 2016

David Ramírez Morán

Confianza y estrategia en las tecnologías de la información

Confianza y estrategia en las tecnologías de la información

Resumen:

El mercado de las tecnologías de la información para su utilización con fines de defensa está experimentando las mismas particularidades que caracterizan el comercio con otros sistemas de armas. Tanto las prácticas comerciales como las diplomáticas asociadas a la contratación de sistemas sensibles empiezan a surgir entre los diferentes actores. Las dudas sobre la fiabilidad de los sistemas, el enorme impacto que puede tener una vulnerabilidad, la falta de flexibilidad de las soluciones cerradas al entorno cambiante y los intereses del comprador están dando lugar a nuevas iniciativas que persiguen la protección de la información.

Abstract:

The market of information technologies for use in defence is experiencing the same particularities that characterize the trade with other arms systems. Both commercial and diplomatic practices related to sensitive system contracting are arising between the different actors. Doubts about systems' reliability, the huge impact a vulnerability may pose, the lack of flexibility of closed solutions to the changing environment and buyer's interests are giving rise to new initiatives on information security.

Palabras clave:

Confianza, tecnologías de la información y comunicaciones, estrategia, soberanía, industria.

Keywords:

Trust, Information and communication technologies, strategy, sovereignty, industry.

Introducción

La actual sociedad ha convertido las tecnologías de la información (informática y comunicaciones) en herramientas imprescindibles para el desarrollo de casi cualquier actividad. Las administraciones públicas, los ministerios de defensa y dentro de estos las Fuerzas Armadas no se pueden abstraer de esta realidad. Deben asumir que forman parte del colectivo de usuarios dependientes de este tipo de servicios. Simultáneamente, los organismos también desempeñan el papel de prestadores de algunos de los servicios relacionados con la sociedad de la información mediante las infraestructuras propias con las que cuentan. Juegan así un doble papel en el que actúan a la vez como clientes y como proveedores de servicios de información.

Las plataformas con las que cuentan las Fuerzas Armadas cada vez incluyen un mayor número de sistemas informáticos para su funcionamiento. Un avión de combate, un buque o un vehículo terrestre actual incorpora varios ordenadores en los que se realizan funciones como la gestión del motor, la comunicación entre los ocupantes o el funcionamiento de los distintos sistemas de combate con los que cuenta la plataforma. Además, cada vez se produce una integración mayor de estos sistemas, por lo que es necesario contar con sistemas de intercomunicación entre todos los elementos. Se puede afirmar, por tanto, que las plataformas cuentan con una infraestructura de tecnologías de la información que las dotan de funcionalidad y comunicaciones.

Si se entienden las infraestructuras como una más de las capacidades con la que es necesario contar para satisfacer las necesidades de las Fuerzas Armadas, será necesaria una política de adquisiciones que permita satisfacer los parámetros requeridos de prestaciones, fiabilidad y costes, a la vez que se aseguran parámetros como la seguridad de suministro, el acceso a las tecnologías y otras restricciones relacionadas con la geopolítica y la geoestrategia. Es sobre estas últimas restricciones sobre las que se desarrolla principalmente el contenido del artículo, tras una breve descripción de distintos conceptos que se van a utilizar posteriormente.

Las infraestructuras como materias primas

Las infraestructuras están formadas por hardware, que consiste en el equipamiento informático y de comunicaciones incluyendo los sistemas de interconexión, y por software, que es el conjunto de instrucciones que al ser ejecutadas en el hardware, dan lugar a los servicios. Dentro del software se pueden hacer varias categorías como son el *firmware*, el sistema operativo, los entornos de propósito general para la ejecución de aplicaciones y las aplicaciones específicas con las que se prestan los servicios en la organización.

En la actualidad, tanto los recursos hardware como ciertos recursos software se han convertido prácticamente en una materia prima sometida a los mismos procesos de mercado que caracterizan a bienes más tradicionales como pueden ser los metales o los minerales. La razón de este cambio de tendencia se debe a que la evolución del mercado ha dado lugar que, en las cadenas de valor de los productos que se proporcionan a los clientes, el valor aportado por la fabricación y distribución de estos bienes intermedios sea marginal.

Se ha implantado para estos activos una dinámica de mercado fundamentada en la reducción de costes. Esto ha sido posible gracias a la estandarización de los sistemas que se ha producido en respuesta a la filosofía de sistemas abiertos que ha caracterizado la evolución de la informática y las comunicaciones desde finales de los años 70 y principios de los años 80. Esta tendencia queda confirmada al comprobar la escasa diferenciación en prestaciones que presentan los modelos del mismo segmento de mercado proporcionados por distintos fabricantes, y la rápida concentración de proveedores, que se han visto reducidos a decenas en el caso del hardware e incluso a menos de una decena en el caso del software.

No cabe duda de que siguen existiendo sistemas de prestaciones muy específicas a los que no resulta de aplicación este modelo. También es cierto que la virtualización de los sistemas (procesado, comunicaciones y almacenamiento, en lo que se denomina actualmente hiperconvergencia) está revirtiendo esta singularidad con la sustitución de los sistemas dedicados por una combinación de hardware de propósito general interconectado y configurado de forma que permita conseguir prestaciones similares a las del sistema dedicado. La diferencia entre uno y otro estriba en una considerable reducción de los costes de producción de los equipos que no se trasladan directamente al usuario final pues el coste del software y los servicios asociados a la configuración, mantenimiento y soporte de estas tecnologías hacen que la reducción en el coste final no sea tan significativa.

Los elementos software que se ven afectados por esta tendencia son los sistemas operativos así como las aplicaciones que se pueden considerar como infraestructuras lógicas de almacenamiento y procesado que dan soporte a la sociedad de la información, véase bases de datos y servidores de aplicaciones. El escaso valor creado por la venta de estos productos contrasta diametralmente con el valor generado por los servicios asociados a su soporte y mantenimiento, que son los que reportan considerables beneficios para los proveedores, ya sea de forma directa o a través de los representantes, intermediarios o distribuidores autorizados. De hecho, el modelo tradicional de adquisición del paquete de software que permite usar ilimitadamente el software una vez comprado está siendo sustituido por modelos de licencia por tiempo limitado, que es necesario renovar de forma periódica para que el sistema siga funcionando. Esta política permite reducir los costes iniciales de adquisición (CAPEX) y orquestarlos en una operación equivalente de financiación mediante

su inclusión en los costes de operación (OPEX).

Estrategia en las tecnologías de la información y comunicaciones

Bajo esta concepción de hardware y software como materia prima de escaso valor añadido, la opción adoptada para su adquisición consiste en acudir directamente al mercado en lugar de desarrollarlo directamente, de modo similar a lo que ocurre con las nuevas fuentes alternativas de hidrocarburos, por ejemplo, cuya explotación no resulta rentable dados los precios a los que se negocian los productos de explotaciones tradicionales en el mercado. Por estos motivos, los países o las empresas ni siquiera se plantean el desarrollo de nuevas plataformas. Van a resultar más caras, al no verse reducido su precio por la experiencia y las economías de escala, y también van a presentar peores prestaciones fruto de un menor conocimiento de la tecnología y de no poder usar los diseños de otros fabricantes por estar protegidos por patentes. Los esfuerzos necesarios se consideran baldíos porque entrar en un mercado establecido como el ya existente es complicado y cuesta encontrar el modelo de amortización de la inversión necesaria.

Esta decisión no está exenta de consecuencias y mientras es cierto que se consigue una rápida cobertura de las necesidades más fundamentales acudiendo al mercado, también se está contribuyendo a su distorsión, reduciéndose el número de opciones disponibles y desapareciendo la investigación en estos componentes. Solo los pocos proveedores supervivientes se encargan del desarrollo y mantenimiento de estas tecnologías, actividad que llevan a cabo enfocándola a sus intereses. De esta forma, además de dominar el mercado, les proporciona una situación de control porque, al depender el resto de tecnologías de las prestaciones de estos elementos, solo prosperarán aquellas nuevas tecnologías que se alineen con los intereses de estos proveedores. También pone en su mano una posición de captura del cliente, tanto por la falta de alternativas como por la necesidad de dar continuidad a todo el ecosistema de aplicaciones basado en las prestaciones de estos elementos.

En caso de surgir problemas con estas tecnologías, afectarán a todos los actores y, dado que solo una empresa tiene la capacidad de ponerles solución por tener el control total del producto, las prioridades bajo las que se solucionarán los distintos problemas vendrán determinadas nuevamente por los intereses del proveedor.

Desde el punto de vista económico, la falta de alternativas también afecta a la competencia en el sector, por lo que el proveedor puede permitirse fijar los precios unilateralmente.

Una cuestión de confianza

La utilización de un hardware y un software específico como infraestructura de los sistemas de información conlleva la responsabilidad de brindar a los proveedores de estos elementos la confianza de que se van a encargar de preservar la privacidad e integridad de la información. De hecho, en principio es un brindis a ciegas que solo se ve respaldado por la falta de existencia de hechos que manifiesten lo contrario. Es fácil demostrar que esta preservación ha fallado cuando se publica una fuga de información, pero es muy difícil si esta fuga no es publicada y hay actores que pueden seguir extrayendo información estratégica sin que el usuario pueda percatarse de ello.

Estas fugas se pueden producir por defectos de diseño o programación que dan lugar a vulnerabilidades que pueden ser explotadas para ganar el acceso ilegítimo al sistema, o bien porque, mediante la creación de una puerta trasera (*backdoor*) el fabricante haya incorporado los medios para facilitar que ciertas personas puedan acceder a estos sistemas.

La elevada complejidad de los sistemas juega en contra del usuario por partida doble. A medida que aumentan las funcionalidades que se proporcionan, aumenta el número de puntos en los que se puede producir ese fallo de programación o diseño. Por otro lado, la mayor complejidad hace que sea muy difícil detectar puertas traseras existentes en el software mediante las técnicas de inspección habituales. Para esto último es necesario en muchos casos incurrir en prácticas no permitidas en las licencias de uso, como la ingeniería inversa de las aplicaciones.

Los riesgos están ahí y eso está motivando que haya actores que desconfíen de las soluciones disponibles en el mercado. Los dos casos más representativos son China y Rusia, como se trata a continuación, aunque otros países también están desarrollando iniciativas motivadas no tanto por los riesgos sino también por motivos económicos y de control de la tecnología.

La piratería también es otro factor importante en lo que respecta a la seguridad de los sistemas. Para poder saltarse las medidas de protección de los sistemas anticopia es necesario utilizar aplicaciones que normalmente se desarrollan en entornos sobre los que no se tiene ningún control. Si bien se saltan las protecciones anticopia, el software instalado en el ordenador para hacerlo puede incluir otras funcionalidades como la introducción de puertas traseras para que las personas que lo desarrollaron puedan acceder libremente a los dispositivos pirateados y, por ende, a la información que contienen. En 2009, la Business Software Alliance (BSA) estimaba en un 67% la cantidad de software pirateada en Rusia.[1]

[1] Seventh Anual BSA/IDC Global Software Piracy Study.
http://portal.bsa.org/globalpiracy2009/studies/09_Piracy_Study_Report_A4_final_111010.pdf

También de acuerdo a la BSA, China lleva varios años ostentando el primer puesto en piratería. A partir de estas cifras resulta bastante significativo el riesgo que ambos países están asumiendo en las infraestructuras.

Iniciativas en la República Popular de China

Con la llegada de Windows 8 y el fin del soporte del sistema operativo Windows XP el Gobierno chino vetó la instalación del sistema operativo Windows en los sistemas gubernamentales[2]. Hasta entonces, China se encontraba dentro del programa por el que se proporciona a gobiernos y otras organizaciones acceso al código fuente del sistema operativo y de las principales herramientas de la empresa. De esta forma, es posible analizar el código para diagnosticar la existencia de errores de diseño o de programación y para comprobar que no existen puertas traseras que permitan el acceso a terceras personas. Al no poder acceder al código fuente consideró que utilizar ese sistema operativo así como las aplicaciones ofimáticas suponía un riesgo para su información.

Por otro lado, en lo que respecta al hardware, en un artículo anterior[3] ya hacía referencia a los dispositivos digitales que China estaba fabricando para hacer frente a la limitación impuesta por Estados Unidos a la exportación de coprocesadores utilizados en sistemas informáticos de procesado de altas prestaciones. En 2002 se creó en China la iniciativa de colaboración público privada denominada BLX para la creación de los microprocesadores denominados inicialmente Godson y actualmente Loongson[4], así como las herramientas necesarias para el desarrollo y diseño de sistemas con estos procesadores. Para la fabricación la empresa no cuenta con fundición propia en la que hacer los chip, por lo que lo subcontrata a STMicroelectronics[5], la empresa de microelectrónica creada en 1987 por la fusión de SGS Microelettronica (Italia) y Thomson Semiconducteurs (Francia) y que tiene actualmente la sede social en Suiza. El dispositivo utiliza una arquitectura MIPS-64, lo que resulta significativo a la hora de instalar un sistema operativo, porque no es compatible con las arquitecturas x86 que utilizan los dispositivos de los líderes del sector, Intel y AMD. Sin embargo, dado que no pueden implementar esta arquitectura por motivos de licencia, han incorporado un traductor binario en el dispositivo que permite la ejecución de aplicaciones desarrolladas para estos dispositivos con rendimientos sólo un 30% por debajo de las

[2] «*China bans use of Microsoft's Windows 8 on government computers*» Reuters, disponible en http://www.reuters.com/article/us-microsoft-china-idUSBREA4J07Q20140520
[3] RAMÍREZ MORÁN David «¿Es la supercomputación una herramienta geopolítica?», 2 septiembre 2015, disponible en http://www.ieee.es/Galerias/fichero/docs_analisis/2015/DIEEEA43-2015_Supercomputacion_DRM.pdf
[4] http://www.loongson.cn/index_en.html
[5] www.st.com

aplicaciones nativas.[6]

Se ha desarrollado un catálogo de productos con los que se cubren las diferentes necesidades en lo que respecta a ordenadores de escritorio, sistemas empotrados como routers y otro equipamiento industrial, lo que proporciona al país una considerable independencia tecnológica.

Ante el veto autoimpuesto en el software y los aplicados a la importación de hardware por EE.UU., la solución adoptada por el Gobierno de la República Popular de China ha sido la de desarrollar un sistema operativo basado en Linux con un objetivo doble. El primero es contar con una herramienta de gran potencia respaldada por la larga historia de éxito de este sistema operativo, que iguala o supera las prestaciones de otras opciones comerciales existentes en el mercado. Por otro lado, el segundo objetivo es contar con un sistema operativo que funciona de forma nativa en los dispositivos que ha desarrollado. Un sistema operativo basado en Linux se puede instalar en arquitecturas muy diversas, incluida la arquitectura MIPS-64 de los dispositivos Loongson. Por tanto, la utilización del sistema operativo Linux en un dispositivo de la familia Loongson permite explotar al máximo la capacidad del dispositivo.

Iniciativas en Rusia

En Rusia, la eliminación del sistema operativo Windows se debe a una política puesta en marcha por Vladimir Putin en 2010 por la que planteaba 2016 como fecha límite para eliminar los equipos cuyo sistema operativo fuera Windows de las administraciones públicas y sustituirlo por software de fuentes abiertas.[7]

El Gobierno ruso afirma que el motivo de desarrollar equipamiento informático propio es el de «sustituir los modelos extranjeros que no garantizan la ausencia de *spyware* o protección contra las fugas de información»[8]. Para ello, en 2014 creó United Instrument Manufacturing Corporation, una filial de la empresa rusa estatal Rostec, en la que se agrupan instalaciones de investigación y producción del sector de la radio y la electrónica.[9]

Recientemente publicaba UIMC la noticia de que próximamente pasará a producción la

[6] Weiwu Hu et al. «Godson-3: A Scalable Multicore RISC Processor with x86 Emulation» IEEE micro. Vol.29 N.2 2009, disponible en http://www.computer.org/csdl/mags/mi/2009/02/mmi2009020017-abs.html

[7] «Putin to put Russian government on Linux by 2015» *Computer World,* disponible en http://www.computerworld.com/article/2511966/government-it/putin-to-put-russian-government-on-linux-by-2015.html

[8] http://www.eng.opkrt.ru/index.php/news/205-uimc-started-developing-equipment-based-on-russian-processor-and-protected-from-cyberespionage

[9] http://www.eng.opkrt.ru/index.php/corporation/about-the-corporation

última versión de su microprocesador Elbrus-8C, que cuenta con 8 núcleos. Se trata de un dispositivo con arquitectura SPARC que, al igual que el dispositivo desarrollado por China, incorpora traductores binarios que permiten la ejecución de instrucciones de las arquitecturas x86 así como de las arquitecturas ARM diseñadas por la empresa inglesa.

Al igual que en el caso de China, el desarrollo de un sistema operativo basado en Linux da esa doble respuesta al problema de permitir contar con un sistema operativo eficiente y que permite explotar al máximo las prestaciones de sus dispositivos por utilizar una arquitectura SPARC, que también se encuentra entre las soportadas por Linux.

Otras iniciativas

Corea del Norte es otro de los países que ha tenido que tomar una iniciativa para contar con tecnologías de la información que le permitan aprovechar las ventajas asociadas. En su caso, se ha optado también por desarrollar un sistema operativo propio basado en Linux, denominado Red Star y del que se han filtrado recientemente informaciones sobre la publicación de la versión 3.[10]

En India, también se está introduciendo una solución de software libre basada en Linux con el sistema operativo Bahrat Operating System Solutions (BOSS)[11], que ya va por su versión 5 desde que fuera lanzado en 2007, y con el que se prevé sustituir el sistema operativo Windows de los ordenadores gubernamentales.

Varios países europeos se han embarcado también en la sustitución de productos comerciales por herramientas de software libre con funcionalidades similares o equivalentes. Por ejemplo, el Ministerio de Interior de Francia ha sustituido las herramientas ofimáticas de Microsoft por herramientas de software libre[12], al igual que está haciendo el Gobierno de Italia[13], que por una ley promulgada en 2012 debe migrar los sistemas gubernamentales a herramientas de software libre, o Polonia con las herramientas de correo electrónico[14]. Holanda es otro de los países en los que el software libre también se está utilizando en el Ministerio de Defensa.[15]

[10] http://www.theguardian.com/world/2015/dec/27/north-koreas-computer-operating-system-revealed-by-researchers
[11] http://trak.in/tags/business/2015/09/15/boss-os-made-in-india-operating-system-boss-replace-microsoft-windows/
[12] https://joinup.ec.europa.eu/community/osor/news/frances-defence-ministry-dutiful-studies-free-software
[13] https://joinup.ec.europa.eu/community/osor/news/italian-military-switch-libreoffice-and-odf
[14] ttps://joinup.ec.europa.eu/community/osor/news/frances-defence-ministry-dutiful-studies-free-software
[15] https://joinup.ec.europa.eu/community/osor/news/open-source-advancing-dutch-defence-ministry

La diplomacia y los mercados tecnológicos

El Gobierno de Estados Unidos hacía público recientemente que se va a implantar el sistema operativo Windows 10 con una configuración optimizada para la seguridad de los terminales en todos sus ordenadores, fijos y portátiles, y tabletas. La motivación que ha conducido a esta decisión es la mayor seguridad que aporta este sistema operativo respecto a versiones anteriores, así como una disminución de costes al reducir el número de sistemas distintos a mantener[16]. Una comunicación de este tipo resulta llamativa pues, mientras en el pasado se ha publicado con frecuencia la instalación de herramientas de software libre en entornos de defensa, el Gobierno de Estados Unidos nunca había informado sobre la actualización de sus sistemas a nuevas versiones del sistema operativo, a excepción del problema que supuso el fin del soporte de Windows XP.[17]

Una noticia en la que se publicita la implantación por parte de un Gobierno de una solución tecnológica desarrollada por una de sus empresas y en la que se ensalzan las virtudes de la tecnología, responde a una de las prácticas que mejor contribuyen a la exportación de tecnologías de defensa. Si además se tienen en cuenta las dificultades que está experimentando la compañía para la adopción de este producto por el gran público, resulta bastante evidente la campaña de apoyo institucional que se está realizando.

Hace unos meses se producía otra noticia en esta misma línea. El Gobierno de Reino Unido anunciaba la migración de los sistemas ofimáticos del Ministerio de Defensa a una solución basada en la nube y proporcionada también por Microsoft: Office 365[18]. En este caso, la barrera a derribar es la reticencia que los gobiernos tienen a que información tan sensible como la que se trata en el Ministerio de Defensa abandone los sistemas propios de la organización y sea custodiada en servidores externos controlados por una empresa. El hecho de que la adopción la realizara Reino Unido puede achacarse a la pertenencia de ambos países a Five Eyes, el acuerdo entre EE.UU, Reino Unido, Canadá, Australia y Nueva Zelanda para compartir información de inteligencia.

[16] http://www.defense.gov/News-Article-View/Article/688721/dod-wide-windows-10-rapid-deployment-to-boost-cybersecurity

[17] GÓMEZ RUEDAS Jesús, «Adiós al soporte a Windows XP en el Ministerio de Defensa: lecciones aprendidas», disponible en http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO18-2015_WindowsXP_Fin_JesusGomezRuedas.pdf

[18] STONE, Mike «IT transformation in the Ministry of Defence», disponible en https://governmenttechnology.blog.gov.uk/2014/08/06/guest-post-it-transformation-in-the-ministry-of-defence/

Las decisiones tomadas por Rusia y China así como su publicación en medios internacionales constituyen un mensaje político bastante contundente. Siembran dudas sobre la fiabilidad de los sistemas a la hora de proteger la información más sensible de los gobiernos y también de las empresas. De hecho, la compañía rusa que fabrica los dispositivos procesadores afirma que el motivo de desarrollar equipamiento informático propio es el de «sustituir los modelos extranjeros que no garantizan la ausencia de *spyware* o protección contra las fugas de información»[19].

Conclusiones

Las tecnologías de la información y las comunicaciones se han convertido en una capacidad fundamental para el funcionamiento de empresas, organizaciones y gobiernos. Dada la importancia que están adquiriendo, las decisiones para su contratación ya no pueden circunscribirse únicamente a los técnicos que tradicionalmente venían seleccionando la mejor alternativa de acuerdo a sus criterios, sino que es necesario aplicar un punto de vista más global que incluye motivaciones estratégicas y de política industrial.

Actualmente el mercado de soluciones está cubriendo las necesidades, aunque puede detectarse cierta carencia de alternativas, que no solo da lugar a situaciones de dependencia de ciertos proveedores, sino que también afectan a la competencia, inexistente en algunos casos.

Existe una tendencia generalizada a utilizar el software libre como solución a la falta de alternativas y a los elevados costes por licencias de las tecnologías comerciales. Hay que asegurarse de que las garantías de estas soluciones sean suficientes para la naturaleza de la información que van a custodiar. En lo que respecta al mayor control que estas tecnologías proporcionan por estar disponible su código para el análisis y revisión, es necesario tener en cuenta que dicho control pasa indefectiblemente por contar con los recursos humanos y técnicos que permitan analizarlo y no depositar esta responsabilidad únicamente en el buen hacer de un tercero.

Las soluciones implantadas actualmente son fruto de largos procesos de desarrollo y ciclos de optimización, lo que dificulta de manera importante la aparición de nuevos actores en el mercado. Sin embargo, se está corriendo un riesgo creciente pues este escalón de entrada va a crecer indefinidamente y supone una pérdida de capacidad de decisión para aquellos que

[19] http://www.eng.opkrt.ru/index.php/news/205-uimc-started-developing-equipment-based-on-russian-processor-and-protected-from-cyberespionage

únicamente actúan como clientes de los proveedores. Algunos países empiezan a tomar medidas al respecto y están sacrificando las prestaciones y la facilidad de acceso a las tecnologías para desarrollar capacidades propias con las que desarrollar conocimiento y hacer frente a una eventual limitación del acceso a las tecnologías.

David Ramírez Morán
Analista del IEEE