El caso Windows

Windows XP ha agotado su ciclo de vida ¿cuáles son las consecuencias?

VOLKER JUNG, ANTHONY BYATT – El exitoso y popular sistema operativo de Microsoft Windows XP tiene ya bastante más de una década. Aunque alrededor del 30 por cierto de los usuarios de Windows aún utilizan XP, un sistema operativo tan antiguo no puede recibir soporte para siempre. Por ello, Microsoft dejó de prestar asistencia al XP el 8 de abril de 2014. Esto implica que no habrá más actualizaciones de seguridad ni nuevos parches ni soporte activo. El efecto de esta medida es que el XP se convertirá en un sistema inseguro, poco fiable e incompatible con el hardware de TI más reciente, como ordenadores, componentes de ordenadores, equipos de redes e impresoras. En otras palabras: el final de la era XP afecta a muchas aplicaciones industriales y requiere una respuesta proactiva de los usuarios.

Hace tiempo, la idea de ejecutar una aplicación industrial sobre Microsoft Windows parecía descabellada. Pero cuando Microsoft presentó su sistema operativo Windows XP hace ya más de una década, la industria tomó nota. Windows XP proporcionaba la estabilidad, la flexibilidad y la funcionalidad que muchos usuarios industriales necesitaban, y pronto se incorporó a todo tipo de aplicaciones imaginables.

Pero todo lo bueno termina: el 8 de abril de 2014 concluyó la era Windows XP, cuando Microsoft anunció el final del soporte para el producto. Por supuesto, Microsoft avisó profusamente y con mucha antelación y las empresas pudieron prepararse para el cambio. Pero aún quedaban muchas preguntas por responder: ¿Un sistema XP independiente podría seguir ejecutándose sin problemas? ¿Qué ocurriría si el sistema XP estuviera integrado en otro sistema? ¿Se necesitaría hardware nuevo y cuál sería su coste en toda la organización? ¿Cuánto costaría el cambio? ¿La virtualización podría resolver el problema? ¿Qué soporte existiría para migrar a un nuevo sistema?

Imagen del título
Microsoft dejó de prestar soporte para XP el 8 de abril de 2014. ¿Cuáles son las repercusiones para los usuarios industriales?

Las respuestas a estas preguntas no siempre fueron sencillas, y pronto quedó claro que el final del soporte para XP sería complicado. Los problemas más importantes pueden agruparse en cuatro categorías:
– Seguridad
– Cumplimiento
– Ausencia de soporte de distribuidores de software independiente
– Soporte de fabricantes de hardware

De ellos, los problemas de seguridad son los más críticos.

Actualizaciones de seguridad de Windows XP

En 2010, el gusano Stuxnet copó los titulares de todo el mundo. Con un tamaño de solo 500 kB, este software malicioso atacó como mínimo a 14 centros industriales de Irán, incluida una planta de enriquecimiento de uranio. Stuxnet atacó en tres fases: primero se dirigió contra redes y equipos de Microsoft Windows, después buscó el software (también basado en Windows) utilizado para programar sistemas de control industrial, y por último penetró en los controladores lógicos programables utilizados para controlar la maquinaria.

Desde Stuxnet, el vulnerable paisaje de la TI industrial sufre constantes ataques cada vez más sofisticados. Por ejemplo, la estrategia de ataque “watering hole” se ha diseñado para introducir malware en los sistemas objetivo. En esta estrategia, la parte maliciosa supone u observa los sitios web que la empresa utiliza con mayor frecuencia, después los infecta y se sienta a esperar que la víctima los visite y descargue inconscientemente malware en su ordenador. Este sistema de ataque estratégico a sitios web pilla a las víctimas por sorpresa, porque los sitios web infectados siempre habían sido de confianza.

Además, el intruso puede manipular perfiles de usuario auténticos de un sistema para dar acceso a extraños. Las configuraciones de los PC también se pueden manipular convirtiéndolos en blanco de, por ejemplo, troyanos de administración remota (RAT), es decir, malware que concede al intruso control administrativo sobre el ordenador objetivo. Los RAT pueden infiltrarse en un ordenador mediante un archivo adjunto a un mensaje de correo electrónico.

1 Sistemas de control/HMI (interfaz hombre-máquina) que deben evolucionar

Sistema/HMI	Comentario
System 800xA	Sistemas centrales 800xA (V5.0 y anteriores)
Freelance	Sistemas Freelance (V6.2 – V9.1)
Generación de energía Portal/Tenore	Todas las versiones basadas en Windows
Conductor NT	Todas las versiones basadas en Windows; la cuenta se hace por el número de servidores, no por el número de sistemas
Process Portal B	Todas las versiones

Una vez infectado el sistema host, el intruso puede usarlo para propagar más RAT y formar un botnet, es decir, un conjunto de ordenadores infectados que se manipulan al unísono para causar más daño.

Dado que un RAT concede control administrativo, permite al intruso vigilar la conducta del usuario con keyloggers u otro spyware, activar una cámara web, acceder a información confidencial, formatear unidades, eliminar o modificar archivos, etc.

En junio de 2014, la familia de malware Havex acaparó los titulares por atacar sistemas de control en diversos ramos de la industria, incluido el sector energético. Uno de los componentes principales de Havex es un RAT. El RAT troyanizó sitios web de fabricantes de sistemas control industrial (ICS) y control de supervisión y adquisición de datos (SCADA). En total, Havex atacó 146 servidores; para ello se utilizaron 88 variantes del RAT Havex y se rastrearon 1500 direcciones IP en un intento de identificar víctimas. Sin duda, Havex fue un ataque grave a la industria.

En julio de 2014, el virus “Energetic Bear” infectó más de 1000 empresas energéticas de Europa y Estados Unidos. Teóricamente, este virus permite a los hackers controlar centrales eléctricas.

Vistos estos ejemplos, es evidente que el entorno de TI industrial es bastante vulnerable, y sin actualizaciones críticas de seguridad de Windows XP, los ordenadores quedan a merced de ataques de virus, spyware y otro software malicioso que puede robar o dañar datos e infor-

2 Estrategias de actualización de XP

Windows XP		Controlador				
800xA	3.1 4.0 4.1 5.0	all	→	800xA	5.1	6.0
Freelance	6.2 7.1 7.2 8.1 8.2 9.1	all	→	Freelance	2013	2015
Conductor NT	all	DCI	→	800xA	5.1	6.0
		Freelance	→	Freelance	2013	2015
			→	800xA	5.1	6.0
		Harmony	→	800xA	5.1	6.0
			→	Symphony +	2.0	
PPB	all	MOD 300	→	800xA	5.1	6.0
		Freelance	→	Freelance	2013	2015
			→	800xA	5.1	6.0
		Harmony	→	800xA	5.1	6.0
			→	Symphony +	2.0	
PGP/Tenore	all	Freelance	→	Freelance	2013	2015
			→	800xA	5.1	6.0
		Harmony	→	800xA	5.1	6.0
			→	Symphony +	2.0	

mación empresarial. El software antivirus ya no proporciona protección total para sistemas XP. Los intrusos podrán utilizar los dispositivos que ejecuten XP como punto de acceso a redes de TI. Esto significa que incluso los ordenadores con sistemas operativos con soporte están en peligro.

Hardware

La mayoría de los fabricantes de hardware informático, impresoras y equipos de red ya han dejado de ofrecer asistencia a Windows XP en hardware nuevo. Esto significa que los controladores de software necesarios para ejecutar Windows XP en este hardware nuevo ya no están disponibles en la mayoría de los casos, es decir, que no habrá controladores de XP para discos duros, impresoras, tarjetas gráficas, equipos de red, etc. nuevos. Comprar un ordenador con sistema XP no será ni fácil ni barato. El hardware basado en XP quedará obsoleto y será difícil de encontrar. Cada vez serán más frecuentes las interrupciones imprevistas provocadas por la falta de componentes de hardware.

Cumplimiento

Puede que las empresas vinculadas al cumplimiento de obligaciones reguladoras, como la Health Insurance Portability and Accountability Act (HIPAA) de Estados Unidos, dejen de poder cumplir los requisitos impuestos si continúan utilizando Windows XP. Con tantos datos personales y confidenciales almacenados actualmente en servidores, la seguridad de los datos es un motivo muy importante de preocupación.

Ausencia de soporte de distribuidores de software independiente

Muchos distribuidores de software ya no podrán prestar soporte a los productos ejecutados sobre Windows XP, puesto que dejarán de recibir actualizaciones de este sistema. Por ejemplo, el nuevo paquete Microsoft Office utiliza el sistema Windows más nuevo y es incompatible con Windows XP.

¿Qué hacer?

Con tantos problemas a la vista, ¿qué debemos hacer? La recomendación de Microsoft y de todas las empresas de seguridad cibernética es actualizar a Windows 7 u 8. Esto incluye a proveedores de sistemas de control distribuido con sistemas de control que ejecutan sistemas operativos Windows XP y anteriores → 1–2.

Por supuesto, puede realizarse una evaluación del coste de mantener seguras las instalaciones de XP frente a los costes de actualización. Seguir con Windows XP requiere mucho mantenimiento, además de herramientas y soporte de empresas de seguridad cibernética especializadas. Algunas de las acciones que deberá acometer son:

- Reducir el tamaño del registro para incluir solo aquellos servicios absolutamente necesarios.
- Utilizar agujeros negros de servidores de nombres de dominios (DNS) para bloquear el acceso al sitio web real.
- Emitir una alerta al detectar una conexión de red virtual o escritorio remoto iniciada en un extremo.
- Prevenir la ejecución binaria para usuarios temporales en el sistema de archivos o emitir una alerta cuando esta se produzca.
- Crear una lista blanca de binarios de servicio en el sistema operativo.
- Emitir una alerta para inicios/detenciones/cambios de servicio.
- Auditar listas de control de acceso, etc.
- Realizar copias de seguridad periódicas del sistema de control.
- Hacer acopio de componentes de TI compatibles.

Conservar Windows XP es cada vez más insostenible. Los avances del software son una parte inevitable de la vida útil de la TI industrial, y pasar de Windows XP a un sistema operativo superior es uno de los más significativos. Este paso permitirá a los usuarios cumplir las demandas de seguridad, hardware, software y cumplimiento del mundo moderno de la TI industrial.

ABB recomienda a los clientes que utilicen sistemas operativos Windows XP que evalúen los planes de ciclo de vida de sus sistemas y la estrategia de mitigación de riesgos. Asimismo, ABB ofrece soluciones para remediar o mitigar riesgos y ayudar a los clientes a proteger mejor sus instalaciones y a su personal, garantizando la seguridad de las operaciones y la continuidad de la producción. Existen servicios que ayudan a satisfacer las necesidades de todos los clientes, incluidos los que no pueden actualizar el sistema de inmediato y los que decidan seguir utilizando Windows XP.

Volker Jung
Process Automation Division
Mannheim, Alemania
volker.jung@de.abb.com

Anthony Byatt
Editorial consultant
Louth Village, Irlanda