CENTRO DE CIBERSEGURIDAD INDUSTRIAL

CÓMO IMPACTA EN EL NEGOCIO EL USO DE SOFTWARE SIN SOPORTE

Ejemplo Windows XP en el mundo industrial

Hoy en día las organizaciones industriales dependen en gran medida de la tecnología para competir en un mercado global, por ello es necesario que el software de operación sea resilente.

Patrocinadores del CCI

Platinum

Telefónica

Gold

Check Point SOFTWARE TECHNOLOGIES LTD.

paloalto NETWORKS

Symantec.

TREND MICRO

Silver

FORTINET

Honeywell

indra

JUNIPER NETWORKS

S21sec

SOURCEfire

pwc

Tecnocom

TSK GRUPO

Bronze

ABS

accenture

everis

EULEN SEGURIDAD

gmv

Intermark it

internet security auditors

IOActive

KASPERSKY lab

LOGITEK

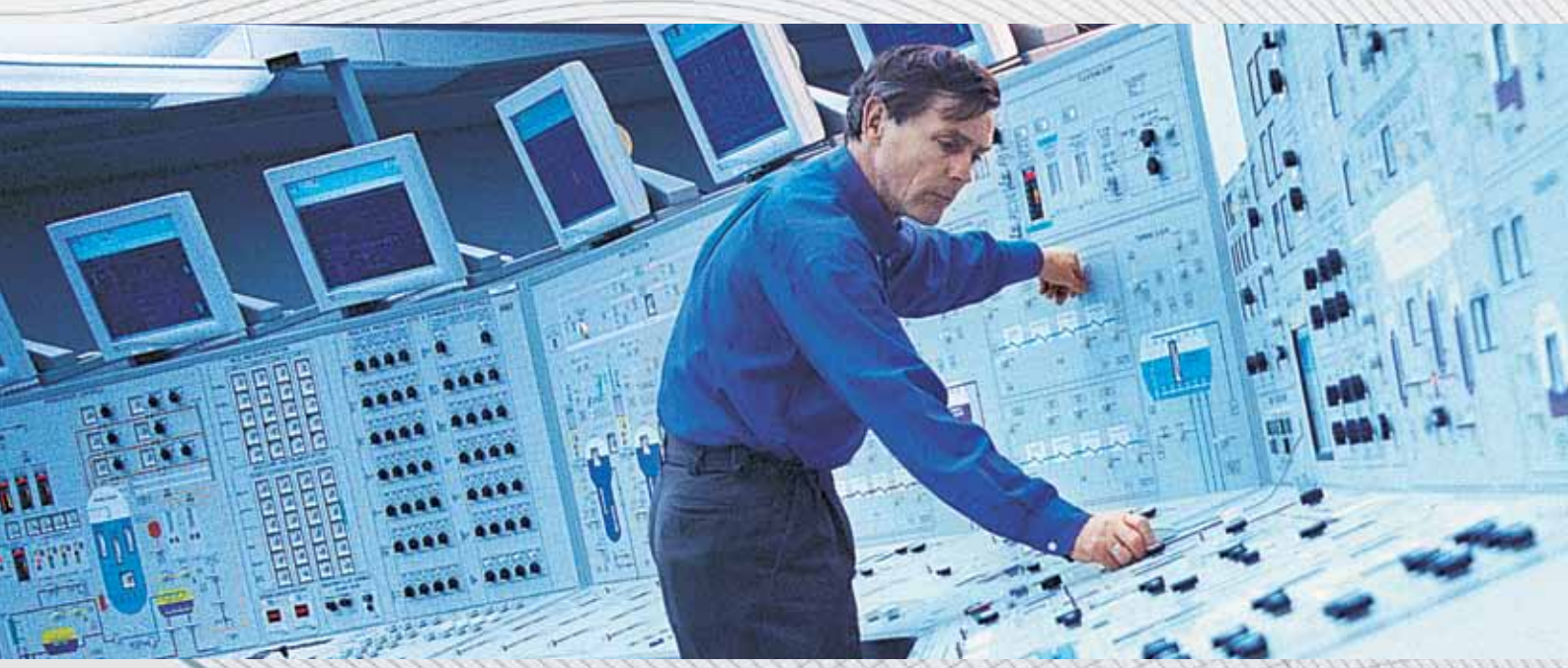
Microsoft

S2 GRUPO

SIEMENS

tecnalia Inspiring Business

TECNICAS REUNIDAS



El Centro de Ciberseguridad Industrial (CCI) es una organización independiente sin ánimo de lucro cuya misión es impulsar y contribuir a la mejora de la Ciberseguridad Industrial desarrollando actividades de análisis, desarrollo de estudios e intercambio de información sobre el conjunto de prácticas, procesos y tecnologías, diseñadas para gestionar el riesgo del ciberespacio derivado del uso, procesamiento, almacenamiento y transmisión de información utilizada en las organizaciones e infraestructuras industriales y cómo éstas suponen una de las bases sobre las que está construida la sociedad actual.

El CCI aspira a convertirse en el punto independiente de encuentro de los organismos, privados y públicos, y profesionales relacionados con las prácticas y tecnologías de la Ciberseguridad Industrial, así como en la referencia hispanohablante para el intercambio de conocimiento, experiencias y la dinamización de los sectores involucrados en este ámbito.

C/ Maiquez, 18 · 28009 MADRID
Tel.: +34 910 910 751
e-mail: info@cci-es.org
www.cci-es.org
Blog: blog.cci-es.org
Twitter: @info_cci

Índice

Introducción 8
Escenario del Software Industrial 10
La pirámide del software de automatización industrial 11
Los sistemas operativos de tiempo real (RTOS) 11
- Rt-11 12
- Núcleo RTOS 12
- LynxOS 12

Los sistemas operativos de proceso, planta y empresa 12
- Microsoft Windows 12
- Unix 13
- GNU/Linux 13
- OS X 13

Despliegue de Windows XP en el mundo industrial 13
Descripción del escenario de Vulnerabilidades y amenazas 14
Seguridad en el ciclo de vida del desarrollo de software industrial 15
- Trustworthy computing de Microsoft 16
- Comprehensive, Lightweight Application Security Process (CLASP) 16
- Software Assurance Maturity Model (SAMM) 17

Inhibidores para la actualización 17
- Falta de homologación 17
- Reticencias al cambio 18
- Costes 18
- Interdependencia con otros sistemas 18
- Desconocimiento 18

Impulsores para la actualización 18
- Productividad 18
- Actualización tecnológica 18
- Reducción de los riesgos de Ciberseguridad 19
- Cumplimiento normativo o requisitos obligatorios del fabricante 19
- Interoperabilidad 19

La respuesta de las organizaciones industriales 19
- Principales razones para la renovación de software 20
- Principales dificultades para migrar software en un entorno industrial 20

Gestión de cambios y parches 22
Impacto para el negocio 24
Recomendaciones.Buenas prácticas 26
Conclusiones 28
Recursos 30

Ilustración 1
Pirámide del software de automatización industrial 11

Ilustración 2
Interfaces 12

Ilustración 3
Porcentaje de equipos desprotegidos (no disponen de protección contra malware en tiempo real) en función de su sistema operativo. 15

Ilustración 4
Porcentaje de equipos protegidos y desprotegidos que han sido infectados en función de su sistema operativo. 15

Ilustración 5
Fases del ciclo de vida del desarrollo de software. 15

Ilustración 6
Coste de la mitigación en las distintas fases del ciclo de vida. 15

Ilustración 7
SAMM 17

Ilustración 8
Parque de equipos Windows XP en el entorno industrial. 19

Ilustración 9
Parque XP actualizado a versiones nuevas. 20

Ilustración 10
Impulsores para la actualización. 20

Ilustración 11
Inhibidores para la actualización. 20

1

Introducción

El concepto de **software industrial** va más allá de los programas o aplicaciones de automatización, también su documentación, datos y el soporte del producto necesario para garantizar el comportamiento adecuado del software, así como eliminar errores, fallos y debilidades de seguridad, es decir, proporcionar un **"software resiliente"** es imprescindible para garantizar las operaciones del negocio.

Normalmente los fabricantes de software producen parches durante el ciclo de vida del producto, y se comprometen a seguir generándolos durante algunos años después del final de la distribución del producto en el mercado. Al final de este ciclo de vida prolongado, el fabricante discontinúa su soporte para el mantenimiento del software, y se detiene toda actividad alrededor de él, una vez que se considera que los clientes han tenido tiempo suficiente para actualizar sus plataformas a los productos más modernos.

La Agencia Europea para la Seguridad de la Información y las Redes (ENISA) advierte sobre los riesgos del uso de software discontinuado, no sólo debido a la falta de apoyo por parte del fabricante, sino también de terceros, como los fabricantes de anti-malware u otro tipo de software o periféricos. Esto dará lugar a la exposición persistente a las vulnerabilidades y la imposibilidad de actualizar los periféricos o aplicaciones de terceros.

En los últimos años ha aumentado significativamente la exposición a los riesgos tecnológicos y por ello ninguna organización industrial que disponga de procesos críticos automatizados mediante tecnología, debería poner en riesgo la operación de su negocio por la falta de soporte.

En este documento presentamos Windows XP, como ejemplo de software donde el fabricante discontinúa su soporte para el mantenimiento del producto, y se detiene toda actividad alrededor de él y lo que puede suceder en una organización industrial que no ha previsto la actualización a una versión de sistema operativo con soporte. También se encontrarán en este documento datos sobre el número de equipos en las organizaciones que todavía cuentan con sistema operativo Windows XP, así como el porcentaje de actualización a versiones más recientes de Microsoft en un entorno industrial, permitiendo tomar conciencia de la exposición a los riesgos tecnológicos por un sistema operativo sobre el que funciona gran parte del software industrial como SCADA, HMI, MES o historiadores entre otros.

Este documento identifica los impulsores y los inhibidores a la hora de realizar las actualizaciones de software, los cuales están basados en una encuesta realizada a organizaciones industriales, ingenierías y fabricantes industriales que tienen aplicaciones industriales que funcionan sobre Windows XP. También en el documento se identifican los principales escenarios de vulnerabilidades y amenazas provocados por las deficiencias en la actualización del software en entornos industriales automatizados y el impacto de una gestión de parches no adecuada.

2

Escenario del Software Industrial

El **software de sistema** tiene como objetivo independizar adecuadamente al usuario y al programador de los detalles físicos del sistema industrial, como son la memoria, el disco, las entradas analógicas y digitales, o los dispositivos de comunicaciones. El software de sistema proporciona al usuario y al programador un interface y herramientas que facilitan el control físico del sistema. Este software se conoce como sistema operativo.

El **software de programación industrial** es el conjunto de herramientas que le permiten al programador desarrollar aplicaciones informáticas con compiladores, intérpretes y plataformas de desarrollo industrial, entre otros.

El **software de aplicación industrial** es aquel que permite a los usuarios llevar a cabo tareas específicas como monitorizar, controlar o adquirir datos de los controladores (SCADA) o almacenar estos datos, como es el caso de los historiadores.

Hoy en día el software, tanto de sistema, como de programación o aplicación requiere una garantía de rendimiento, funcionalidad, interoperabilidad y seguridad para evitar errores, debilidades y fallos. Cuanto más crítica es la operación que realiza el software, más importante debe ser su capacidad de resistencia. Debemos entender que en un entorno tan complejo y conectado como el actual, el software tiene que evolucionar hacia la prestación de un servicio resiliente por parte de los fabricantes de software.

LA PIRÁMIDE DEL SOFTWARE DE AUTOMATIZACIÓN INDUSTRIAL

En el entorno industrial tenemos software en distintos niveles. Cada una de las capas de software deberá interactuar tanto con el nivel o capa inferior de la pirámide, como con el nivel o capa superior. En la imagen encontramos los cuatro niveles en los que se requiere software. El nivel instrumentación, no está representado, se corresponde con el hardware de sensores y actuadores y estaría por debajo del nivel denominado **Campo**, siendo esta la primera capa de software desde la cual se realiza el control básico de las señales de los instrumentos del proceso industrial, en este nivel los sistemas operativos que se utilizan normalmente son RTOS (Sistemas operativos de tiempo real) que controlan el proceso y convierten las señales en datos que son transmitidos al software de la capa de **Proceso** desde donde se realizará la monitorización y supervisión del proceso.

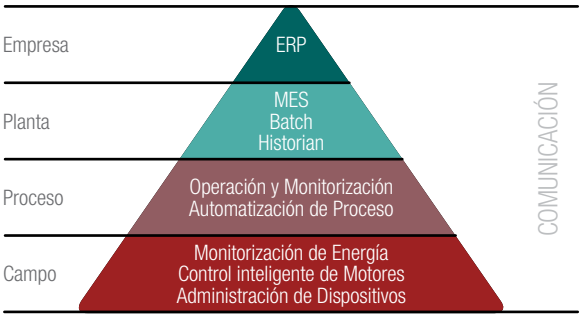


Ilustración 1 – Pirámide del software de automatización industrial

En la capa de **Planta** se encuentran las aplicaciones que se encargarán de facilitar el análisis de los datos obtenidos en la capa de proceso y la información logística, de almacén entre otras obtenidas de la capa **Empresa**.

El software instalado en cada una de estas capas y su comunicación deben ser **resilientes** para garantizar la operación del proceso industrial y la información que constituye el know-how del negocio.

LOS SISTEMAS OPERATIVOS DE TIEMPO REAL (RTOS)

Los sistemas operativos de tiempo real se utilizan en la capa de campo y han sido desarrollados de forma específica para poder ejecutar aplicaciones de tiempo real. Como tal, se les exige corrección en sus respuestas bajo ciertas restricciones de tiempo. Si no las respeta, se dirá que el sistema ha fallado. Para garantizar el comportamiento correcto en el tiempo requerido se necesita que el sistema sea predecible. Sus principales características son la utilización de procesadores predecibles, que cumplan con los plazos de tiempo de ejecución de las tareas, servicios o interrupciones, el uso de poca memoria, la multi-arquitectura, es decir, que su código pueda ser portado a cualquier CPU y que cualquier evento en el soporte físico pueda hacer que se ejecute una tarea.

En estos sistemas operativos suele utilizarse conexiones o redes deterministas CAN Bus o puertos serie RS-232 o RS-485.

RT-11

Es un pequeño sistema operativo de tiempo real, monousuario, para la familia de computadoras de 16 bits PDP-11, de la Digital Equipment Corporation. Fue implementado por primera vez en 1970 y se utilizó ampliamente para sistemas de tiempo real, control de procesos y adquisición de datos a través de la línea completa de computadoras PDP-11.

Núcleo RTOS

Es un sistema operativo en tiempo real que incluye un conjunto de herramientas creadas por la División de Sistemas Embedded de Mentor Graphics para diversas plataformas. Núcleo RTOS es un software embebido y se estima que hay unos 2.110 millones de dispositivos de este tipo en todo el mundo. El desarrollo se realiza normalmente en un equipo host que ejecuta Windows o Linux. Las aplicaciones se compilan para ejecutarse en diversas arquitecturas de CPU. Este sistema operativo se puede encontrar en los controladores de procesos industriales de Honeywell.

LynxOS

Es un sistema operativo de tiempo real tipo Unix de LynuxWorks (anteriormente "Lynx Real-Time Systems"). Las primeras versiones de LynxOS se crearon en 1986, para un procesador Motorola 68010. En 1988-89, una versión de LynxOS se hizo para una arquitectura Intel 80386. Este sistema operativo es utilizado por el fabricante Rockwell.

LOS SISTEMAS OPERATIVOS DE PROCESO, PLANTA Y EMPRESA

Los sistemas operativos para el resto de capas de la pirámide de automatización son los encargados de gestionar los recursos del hardware, hecho que libera a los programadores de aplicaciones de la gestión de todos esos detalles, proporcionando un API (Aplication Programming Interface) de servicios que permite escribir en pantalla, leer del teclado, gestionar el almacenamiento o las comunicaciones. La mayoría de los dispositivos electrónicos que utilizan microprocesadores para funcionar, llevan incorporado un sistema operativo. El sistema operativo de proceso, planta y empresa es manejado mediante un interfaz de usuario, que puede ser gráfico o mediante línea de comandos.

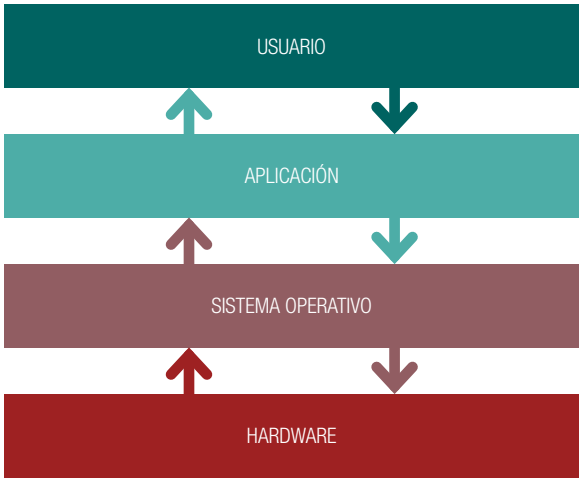


Ilustración 2 - Interfaces

Los sistemas operativos industriales actuales se diseñan y construyen con tres tendencias:

1. Adaptarse rápidamente al hardware de nuevas tecnologías.

2. Maximizar la representación de contenidos en diferentes fuentes de entradas/salidas.

3. Extender la experiencia de usabilidad.

Microsoft Windows

Es el nombre de una familia de sistemas operativos desarrollados y vendidos por Microsoft desde el 25 de noviembre de 1985, llegando a dominar el mercado mundial de las computadoras personales, con más del 90% de la cuota de mercado y ser uno de los software más extendido en los sistemas industriales.

En octubre del año 2001, Microsoft lanzó **Windows XP**, una versión basada en la arquitectura de Windows NT proveniente del código de Windows 2000, incorporando mejoras en la estabilidad y el rendimiento frente a los sistemas anteriores. En dos ediciones distintas, «Home» y «Professional», el primero carece por mucho de la seguridad y características de red de la edición Professional. En enero de 2002 Microsoft comercializa la versión Windows XP embedded, que

es utilizada por fabricantes industriales, como es el caso de Siemens para las versiones SIMATIC PC, por sus ventajas, como vigencia a largo plazo o no requerir activación de licencias.

Durante su existencia se han publicado tres Service Packs, el Service Pack 1 se publicó en 2002, incorporando la utilidad para configurar acceso y programas, soporte de discos de 120 GB y USB 2.0. El Service Pack 2 se publicó en 2004 para corregir errores e incorporar un centro de seguridad, soporte wi-fi y bluetooth entre otros servicios. El Service Pack 3, que se publicó en 2008, incorporaba actualizaciones independientes y una actualización acumulativa de los paquetes anteriores. El soporte estándar para Windows XP finalizó el 14 de abril de 2009. El soporte estándar para Windows XP finalizó el 14 de abril de 2009. El soporte extendido finalizará el 8 de abril de 2014 para Windows XP profesional y el 12 de enero de 2016 para Windows XP embedded, utilizada como hemos mencionado en el mundo industrial.

Las últimas versiones que existen a fecha de publicación de este documento son Windows 8.1 para distintas plataformas (tabletas, 2 en 1, portátiles, equipos de sobremesa, convertibles, AIO, etc.), Windows Server 2012 para servidores y Windows Phone 8 para dispositivos móviles.

Unix

Es un sistema operativo portable, multitarea y multiusuario; desarrollado en 1969, por un grupo de empleados de los laboratorios Bell de AT&T.

El sistema, junto con todos los derechos fueron vendidos por AT&T a Novell, Inc. quien vendió posteriormente el software a Santa Cruz Operation en 1995, y esta, a su vez, lo revendió a Caldera Software en 2001, empresa que después se convirtió en el grupo SCO. Sin embargo, Novell siempre argumentó que solo vendió los derechos de uso del software, pero que retuvo el copyright sobre "UNIX®". En 2010, y tras una larga batalla legal, UNIX ha pasado nuevamente a ser propiedad de Novell.

GNU/Linux

es el término empleado para referirse a la combinación del núcleo o kernel libre similar a Unix denominado Linux con el sistema GNU. Su desarrollo es uno de los ejemplos más prominentes de software libre; todo su código fuente puede ser utilizado, modificado y redistribuido libremente por cualquiera bajo los términos de la GPL (Licencia Pública General de GNU, en inglés: General Public License) y otra serie de licencias libres.

OS X

Es un sistema operativo basado en Unix, desarrollado por Apple Inc. Ha sido incluido en su gama de computadoras Macintosh desde el año de 2002. La versión 8 OS X es el sucesor del Mac OS 9 (la versión final del Mac OS Classic), el sistema operativo de Apple desde 1984. Está basado en BSD, y se construyó sobre las tecnologías desarrolladas en NeXT entre la segunda mitad de los 80's y finales de 1996, cuando Apple adquirió esta compañía. Desde la versión Mac OS X 10.5 Leopard para procesadores Intel, el sistema tiene la certificación UNIX 03.12.

DESPLIEGUE DE WINDOWS XP EN EL MUNDO INDUSTRIAL

Windows XP se utiliza en la automatización de aparatos médicos, cajeros automáticos, sistemas de control industrial, e incluso en el hardware utilizado en los lectores de tarjetas de crédito.

Muchas organizaciones y fabricantes de software han desarrollado sus aplicaciones solo compatibles con Windows XP. Reconstruir esto es caro y arreglar los problemas de la nueva versión puede llevar tiempo.

En el informe Creating a Timeline for Deploying Windows 7 and Eliminating Windows XP, de Gartner, publicado en 2011 se advierte que muchos componentes hardware y software no funcionarán en Windows XP siendo soportados únicamente en versiones Windows 7 y Windows 8.

La gran mayoría de los fabricantes industriales han desarrollado software de monitorización, control, historiadores y pasarelas de comunicación sobre Windows XP, y la mayoría llevan varios meses recomendando que se actualice a nuevas versiones del sistema operativo para aumentar la productividad, mejorar la seguridad y protección y permitir la compatibilidad con el nuevo hardware y software.

Como ejemplo, Honeywell recomienda la actualización a los usuarios de su sistema SCADA Experion PKS y la solución TotalPlant que funcionan sobre Windows XP, y están sujetas a los riesgos de una versión Microsoft no soportada. Honeywell ofrece apoyo y material para actualizar Windows XP. Consideran que "los riesgos y los costos totales asociados a un fallo cibernético son muy superiores a quedarse en Windows XP". Las vulnerabilidades de un software sin soporte pueden dar lugar a que un virus u otro malware logre explotarlas comprometiendo de esa manera la seguridad de los sistemas.

También OSISoft recomienda la actualización de Windows XP a versión mas reciente de su software PI, uno de los software de almacenamiento y análisis de datos de operación más implantados en el mundo industrial. Entre las razones que OSISoft argumenta para actualizar el sistema operativo están los problemas de seguridad y el riesgo de las vulnerabilidades conocidas y desconocidas que aparecerán y no permitirán aplicar parches para resolverlas.

DESCRIPCIÓN DEL ESCENARIO DE VULNERABILIDADES Y AMENAZAS

El escenario tecnológico actual vive un alto grado complejidad, expansión vertiginosa, e hiperconectividad, que está siendo aprovechado por sofisticadas amenazas. La continua aparición de nuevas piezas de malware, y el desarrollo de nuevas técnicas de explotación es un proceso acumulativo que obliga a los desarrolladores de software a realizar un ejercicio continuo de actualización y mejora de sus programas con el fin de tratar de mantener la seguridad de los mismos. Hoy en día los sistemas operativos y las aplicaciones requieren ser prestadas como un servicio resiliente que se adapte a la complejidad, al crecimiento y a los requisitos de seguridad para combatir las amenazas y las vulnerabilidades garantizando la interoperabilidad, la disponibilidad e integridad en la operación y la confidencialidad de la información que manejan.

Según el informe "Mitigating Risk: Why Sticking with Windows XP Is a Bad Idea" de IDC, la mayoría del software comercial contiene entre 3 y 10 fallos por cada 10000 líneas de código , y que entre el 1 y el 5 % de éstos fallos dan lugar a vulnerabilidades. Eso equivale aproximadamente a una vulnerabilidad por cada 2.000 líneas de código.

Poniendo como ejemplo Windows XP, que contiene aproximadamente 40 millones de líneas de código, se han publicado poco más de mil vulnerabilidades en la National Vulnerability Database (http://nvd.nist.gov), podemos decir que Windows XP tiene una vulnerabilidad por cada 40.000 líneas de código, lo que significa que es un software con un buen nivel de seguridad con respecto a la media del software comercial.

En el ámbito industrial de sistemas SCADA y sistemas de control industrial conocemos un número relativamente pequeño de las revelaciones en estos últimos años, ya que los investigadores de seguridad han comenzado hace relativamente poco tiempo a investigar estos productos. Una vez que los productos SCADA / SCI sean expuestos al escrutinio de seguridad generalizada, puede producirse una avalancha de vulnerabilidades , lo que ocasionará la necesidad de instalar parches en los sistemas de control con mayor frecuencia.

Existe la posibilidad de que existan programas maliciosos a la espera para realizar ataques remotos que se aprovechen de los fallos de seguridad no publicados y los utilicen en el momento que haya finalizado el ciclo de vida de Windows XP. Esto implica que cualquier organización industrial estaría desprotegido por tiempo indefinido ante este tipo de ataques.

Uno de los efectos de mantener en producción software antiguo o no actualizado es el aumento de la ventana de vulnerabilidad tanto en el tiempo que los programas son vulnerables, como en la cantidad de las amenazas que existen sobre ellos.

Cualquier red industrial que disponga de un solo sistema operativo Windows XP estará en riesgo, ya que una vez comprometido ese equipo podrá ser utilizado como plataforma para infectar al resto de equipos independientemente de la tecnología de su sistema operativo.

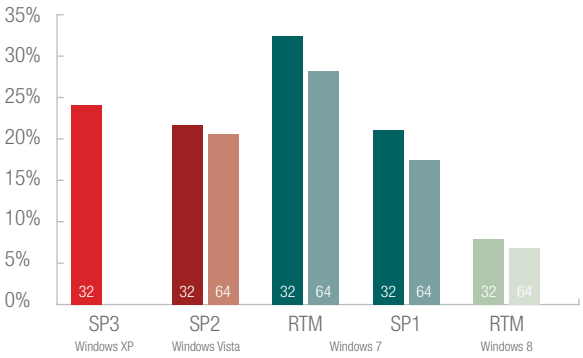


Ilustración 3 - Porcentaje de equipos desprotegidos (no disponen de protección contra malware en tiempo real) en función de su sistema operativo.

Según la anterior gráfica podemos concluir que las versiones antiguas, como Windows XP, o las versiones de sistemas operativos que no tienen instalado el último Service Pack tienen un grado de exposición muy elevado y por lo tanto, ponen en riesgo al negocio, no cumpliendo con la actual necesidad de "Software Resiliente".

Es necesario un mantenimiento muy diligente de los programas, en el que deben colaborar tanto el fabricante como el usuario. Esto no es sencillo de lograr, ya que existen múltiples condicionantes que se detallarán en el siguiente apartado de este documento.

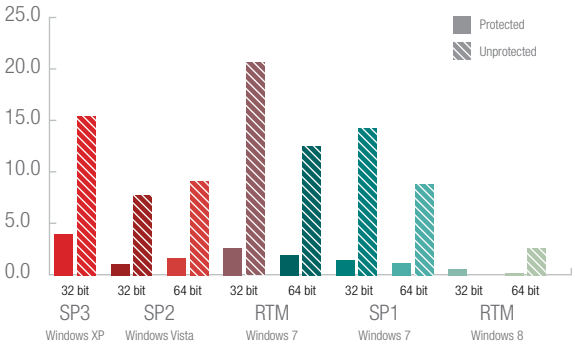


Ilustración 4 - Porcentaje de equipos protegidos y desprotegidos que han sido infectados en función de su sistema operativo.

Como se observa en esta gráfica, los equipos protegidos pueden sufrir infecciones, pero la probabilidad de sufrirlas por no estar protegido aumenta en un 400%, sobre todo en versiones de 32 bits antiguas como Windows XP.

Según el CCN-CERT (CERT del Centro Criptológico Nacional) los sistemas sin soporte se convierten en un "blanco fácil" para explotar vulnerabilidades una vez dejen de publicarse actualizaciones de seguridad por parte del fabricante, y los atacantes y creadores de código dañino se centrarán especialmente en estos sistemas, con la certeza de que a partir del día que dejan de ser soportados ninguna vulnerabilidad será parcheada y sus ataques tendrán siempre éxito.

También el CCN-CERT avisa que después de la publicación por parte de Microsoft de actualizaciones de seguridad para Windows 8 y Windows 7, los atacantes podrían realizar ingeniería inversa de los mismos para comprobar qué vulnerabilidades son parcheadas y comprobar si las mismas están presentes en Windows XP. En caso de ser así, el atacante tendría garantizado el éxito de una posible intrusión a un sistema con Windows XP.

SEGURIDAD EN EL CICLO DE VIDA DEL DESARROLLO DE SOFTWARE INDUSTRIAL

Existen distintos modelos de Ciclo de Vida del Software, que determinan cuales son y de qué manera se ejecutan las etapas del desarrollo de software. Cada modelo presenta sus propias características y alcances de estas etapas.

Ilustración 5 - Fases del ciclo de vida del desarrollo de software.

Es demasiado habitual que no se contemplen requisitos de seguridad en el ciclo de vida del desarrollo del software o se tengan en cuenta en las etapas finales, lo que provoca un sobrecoste en tiempo y esfuerzo para resolver los problemas de seguridad, puesto que ocasionaran rediseño o modificación de gran cantidad de código. Está comprobado que cuanto antes se encuentre una debilidad o fallo en el ciclo de vida del desarrollo de software, más rápida, eficiente y económica será su mitigación, tal y como podemos ver en la siguiente gráfica.

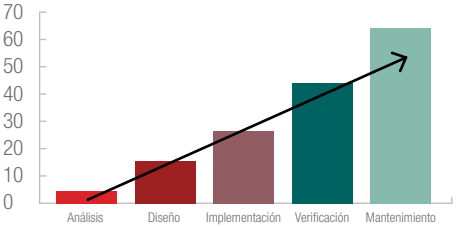


Ilustración 6 - Coste de la mitigación en las distintas fases del ciclo de vida.

Es fundamental involucrar a especialista en seguridad en cada una de las etapas del ciclo de vida del desarrollo del software para incorporar requisitos de seguridad que complementen los requisitos de funcionalidad. La mejor forma de lograr cubrir las exigencias actuales de seguridad en el software industrial está en implementar procesos que proporcionen mayor seguridad, pero que sobre todo se pueda medir. Estos procesos deben minimizar el número de vulnerabilidades de seguridad presentes en el diseño, la programación y la documentación, así como detectarlas y eliminarlas cuanto antes en el ciclo de vida de desarrollo. La necesidad de disponer de seguridad es mayor para el software industrial que procesa información procedente de Internet o redes externas o controla sistemas de gran importancia que pueden sufrir ataques.

Existen varias iniciativas y metodologías para implementar la seguridad en el ciclo de vida del desarrollo de software aplicable al software industrial, algunas de las más extendidas son:

1. Trustworthy computing de Microsoft

2. Comprehensive, Lightweight Application Security Process (CLASP)

3. Software Assurance Maturity Model (SAMM)

Trustworthy computing de Microsoft

Es un proceso que Microsoft utiliza para desarrollar software que pueda resistir ataques malintencionados. Este proceso incorpora varias actividades y materiales relacionados con la seguridad a cada una de las fases del proceso de desarrollo de software de Microsoft. Estas actividades y materiales incluyen el desarrollo de modelos de amenazas durante el diseño de software, el uso de herramientas de exploración del código de análisis estático durante la implementación y la realización de revisiones del código y pruebas de seguridad durante una "campaña de seguridad".

Antes del lanzamiento de software sometido al Software Development Life Cycle (SDLC), un equipo independiente del grupo de desarrollo debe realizar una revisión final de seguridad. En comparación con el software que no se ha sometido al SDLC, el software que ha seguido este proceso ha presentado una reducción considerable en el número de detección externa de vulnerabilidades de seguridad.

La experiencia de Microsoft en seguridad del software real ha permitido establecer una serie de principios de alto nivel para lograr un software más seguro. Microsoft hace referencia a estos principios como SD3+C: Seguro por diseño, Seguro por definición, Seguro en distribución y Comunicaciones. A continuación, incluimos una breve definición de estos principios:

- **Seguro por diseño**: la arquitectura, el diseño y la implementación del software se deben realizar de manera que proteja tanto el software como la información que procesa, además de poder resistir ataques.
- **Seguro por definición**: en el mundo real, el software no es nunca totalmente seguro, por lo que los diseñadores deben asumir que habrá errores de seguridad. Para minimizar los daños que se producirán cuando los atacantes descubran estos errores, el estado predeterminado del software debe elegir las opciones más seguras. Por ejemplo, el software debe ejecutarse con los mínimos privilegios necesarios y los servicios y las características que no sean necesarios de manera habitual deben deshabilitarse de manera predeterminada o establecer que sólo unos pocos usuarios puedan tener acceso a ellos.
- **Seguro en distribución**: se debe incluir con el software información y herramientas que ayuden a los administradores y a los usuarios a utilizar este software con seguridad. Además, la implementación de las actualizaciones debe ser sencilla.
- **Comunicaciones**: los programadores de software deben estar preparados para detectar las vulnerabilidades de seguridad del producto y deben comunicarse de manera abierta y responsable con los usuarios y los administradores para ayudarles a tomar las medidas de protección adecuadas (como la actualización o la implementación de soluciones alternativas).

Comprehensive, Lightweight Application Security Process (CLASP)

Es un conjunto de 24 actividades a desarrollar, 7 roles asociados al SDLC y 104 errores de seguridad asociados a 5 categorías. Está diseñado para ayudar a los equipos de desarrollo de software a construir la seguridad en las primeras etapas del ciclo de vida del desarrollo de software de forma estructurada, repetible y medible.

Se basa en un trabajo de campo muy completo en el que se descompusieron los recursos del sistema de muchos ciclos de vida de desarrollo para crear un conjunto completo de requisitos de seguridad. Estos requisitos resultantes forman la base de las mejores prácticas que pueden permitir a las organizaciones tratar sistemáticamente las vulnerabilidades.

Software Assurance Maturity Model (SAMM)

SAMM es un marco abierto que permite ayudar a las organizaciones a formular y aplicar una estrategia para dotar de seguridad al software mitigando los riesgos a los que se enfrenta una organización. SAMM ayudará a evaluar las prácticas de seguridad existentes, construir un programa en ciclos bien definidos, así como definir y medir las actividades relacionadas con la seguridad.

Por cada una de las etapas del desarrollo del software SAMM define objetivos, actividades, resultados, umbrales de satisfacción, coste, personal, niveles relacionados y métricas.

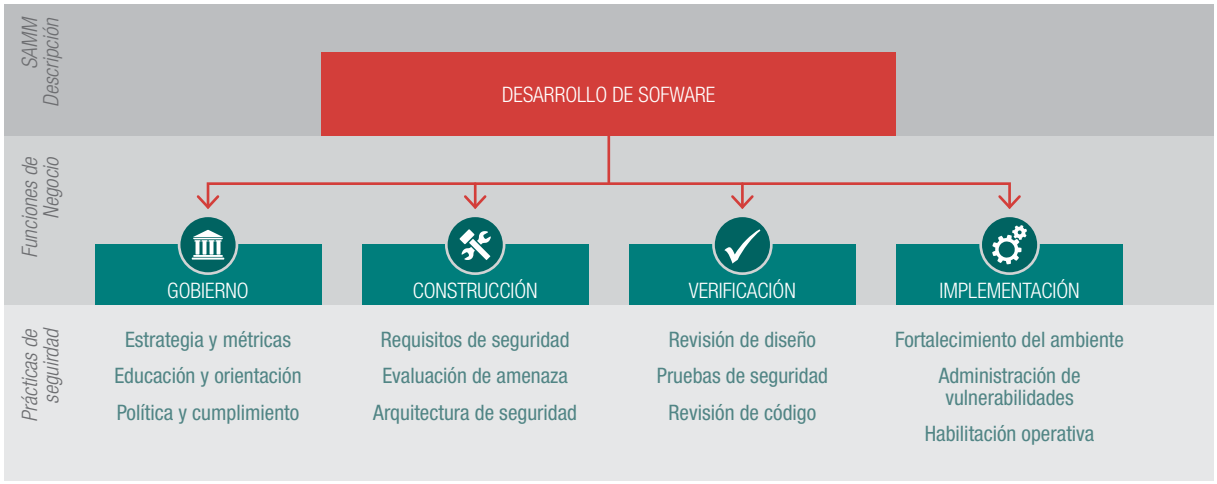


Ilustración 7 - SAMM

INHIBIDORES PARA LA ACTUALIZACIÓN

Falta de homologación

Es práctica habitual que los fabricantes de sistemas industriales homologuen sólo ciertas versiones de software para funcionar con sus sistemas. Esto supone uno de los principales inhibidores para la actualización de software en estos entornos. Mediante la homologación de sólo ciertas versiones de software, los fabricantes garantizan que sus sistemas funcionarán correctamente y que los procedimientos de resolución de incidencias funcionarán de manera óptima, lo cual es fundamental para garantizar la continuidad y el correcto funcionamiento de los procesos que dependen de los sistemas de control industrial. La contrapartida es que el usuario no tiene permitido la aplicación de parches o la actualización del software, bajo el riesgo de incumplir el contrato de mantenimiento con los fabricantes. Esto causa que el software utilizado sea vulnerable a las amenazas aparecidas tras la edición de esa versión particular del software. Este hecho, unido a los largos periodos de amortización de los sistemas (y software) utilizado en los entornos industriales, convierte en potencialmente vulnerables a una gran parte del parque software utilizado en estos entornos.

Según la encuesta que se ha realizado a organizaciones industriales, ingenierías y fabricantes industriales, en el **24%** de las ocasiones la falta de homologación es la razón de no actualizar las versiones de software obsoletas.

Reticencias al cambio

En el entorno de sistemas industriales es frecuente que los usuarios finales y el fabricante de software sean reticentes a los cambios que podrían incidir en el mal funcionamiento provocando problemas graves o difícil de solventar con un impacto económico para el negocio o de calidad importantes en el producto o servicio.

Según la encuesta realizada a los principales actores, en el **40%** de las ocasiones las organizaciones industriales no actualizan para no detener o afectar al proceso de producción. La reticencia al cambio es el factor de freno más importante que se produce actualmente.

Costes

La actualización de software en el mundo industrial tiene un coste de planificación, pruebas y despliegue, además del software, hardware, recursos y costes previos muy superiores a los costes que existen en el entorno corporativo, debido principalmente a tratarse de sistemas críticos para el negocio donde las ventanas de intervención afectan directamente a la producción con los costes de parada pertinentes.

En la encuesta realizada, el inhibidor del coste influye en un **24%** de las ocasiones.

Interdependencia con otros sistemas

En el entorno industrial encontramos distintos niveles de software que requieren la interconexión, dispositivos de campo con proceso, proceso con planta o planta con ámbito corporativo. Un ejemplo de esta interdependencia es el caso de los servidores OPC que permiten la comunicación del nivel de instrumentación con el de campo independientemente de la tecnología de instrumentación, o controladores de campo con aplicaciones del nivel de proceso. Esta interdependencia que se produce en mayor medida en un DCS (Sistema de control distribuido) puede dificultar o incluso impedir la actualización del software del sistema operativo o de la aplicación.

Desconocimiento

La automatización de los procesos industriales es un campo donde la participación de los fabricantes industriales es muy alta, desde el momento inicial del diseño del proyecto, hasta incluso la operación en algunos casos y el mantenimiento en todos los casos. Este elevado nivel de intervención del fabricante provoca en no pocas ocasiones cierto desconocimiento de la propia organización de su propia infraestructura, haciendo que los sistemas, las aplicaciones y sus comunicaciones se conviertan en una caja negra para el personal de ingeniería y técnico de la organización industrial, suponiendo un motivo importante para el retraso de la actualización del software.

Según la encuesta realizada, esto ocurre solo en un **12%** de las ocasiones.

IMPULSORES PARA LA ACTUALIZACIÓN

Productividad

Los costes de productividad por mantener equipos y sus sistemas operativos más antiguos son elevados según el informe **“Mitigating Risk: Why Sticking with Windows XP Is a Bad Idea”**, en este estudio se ha detectado que en los PC con más de cinco años de antigüedad que ejecutan Windows XP, los costes de productividad de los usuarios por PC y por año casi se duplica. Estos mayores costes fueron causados por varios problemas, no todos atribuibles directamente al sistema operativo, pero es común en las soluciones de mayor antigüedad que requieren mas intervenciones y soporte helpdesk, lo cual ocasiona mayores tiempos de inactividad debido a problemas de seguridad, a la espera de respuesta desde atención a usuarios, y al tiempo dedicado a la resolución de los problemas.

En el mundo industrial es habitual agotar la vida del hardware y software. La automatización industrial normalmente contempla periodos de amortización superiores a los 15 años, y el cambio tecnológico suele producirse únicamente cuando la eficiencia y el rendimiento del proceso productivo no es el esperado.

Según la encuesta realizada en el **46%** de los casos la razón para realizar actualizaciones es la inestabilidad en la producción o costes de productividad.

Actualización tecnológica

Los fabricantes de tecnología industrial están acostumbrados a manejar renovaciones tecnológicas con mayor lentitud que los fabricantes de tecnología

corporativa. Desde hace unos años en el mercado de la tecnología industrial se están introduciendo los sistemas MES (Manufacturing Execution System) que permiten analizar los datos de ejecución del proceso de fabricación junto a la información del resto de procesos de la organización, como compras, almacén, logística permitiendo mejorar la eficiencia, rentabilidad y productividad. En estas situaciones o por la necesidad de nuevos requisitos funcionales o de hardware soportado se requiere una actualización tecnológica que impulsa la renovación de los sistemas operativos.

Reducción de los riesgos de Ciberseguridad

En el software discontinuado los usuarios finales no pueden comprobar la integridad del software, ya que los certificados de firma pueden caducar o no ser válidos, este sería el caso si la última distribución original fue firmado por el fabricante. También puede no ser posible verificar la integridad del paquete de software y por tanto estar expuesto a malware o incluso sistemas potencialmente infectados pueden transmitir la infección a través de toda la red.

Estos son algunos de los riesgos que forman parte de los criterios de una organización industrial a la hora de decidir actualizar el software a una versión con soporte, pero desgraciadamente esto solo ocurre en unas pocas organizaciones concienciadas con los riesgos de Ciberseguridad. En el **78%** de las organizaciones no se contemplan a día de hoy estos riesgos para determinar la necesidad de actualizar el software, tal y como se deduce de la encuesta realizada.

Cumplimiento normativo o requisitos obligatorios del fabricante

Los requisitos regulatorios o los del propio fabricante de hardware y/o software industrial se convierten en algunas ocasiones en determinantes a la hora de decidir actualizar el software del sistema operativo. En el **27%** de las organizaciones se contempla como determinantes estos requisitos para actualizar el software.

Interoperabilidad

La interoperabilidad se considera un factor muy bajo a la hora de decidir actualizar el software. En la encuesta realizada tan solo un **5%** de las organizaciones consideran la necesidad de actualizar por garantizar la interoperabilidad como un criterio.

LA RESPUESTA DE LAS ORGANIZACIONES INDUSTRIALES

A menos de 15 días de que Microsoft deje de soportar Windows XP, el **75%** de las organizaciones industriales cuentan con más de 50 equipos que aún tienen el sistema operativo Windows XP y que se utilizan para controlar, monitorizar o almacenar datos de algún proceso industrial.

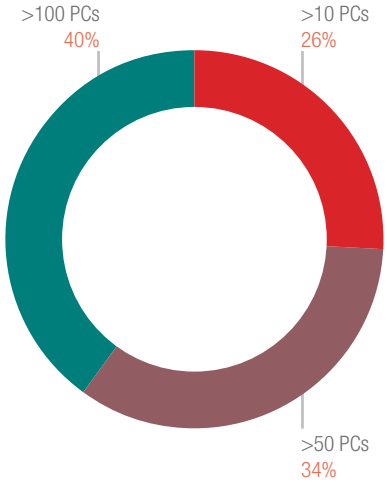


Ilustración 8 - Parque de equipos Windows XP en el entorno industrial

Son menos del **10%** de las organizaciones las que han actualizado completamente su parque de equipos XP a una versión más nueva de sistema operativo. Esto nos indica que se puede actualizar, aunque ello requiera de un esfuerzo previo de planificación y un coste en software y recursos.

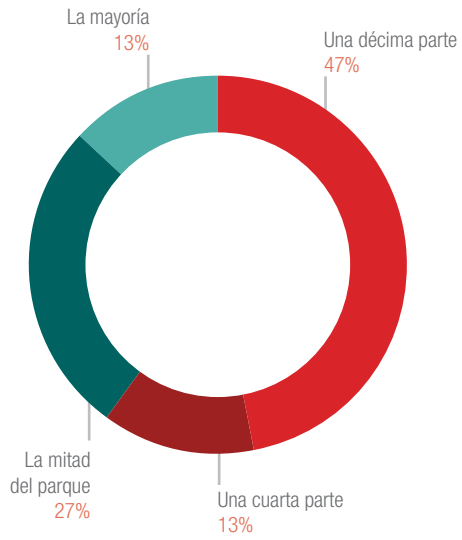


Ilustración 9 - Parque XP actualizado a versiones nuevas

Por otro lado nos encontramos que casi un **50%** de las organizaciones solo han actualizado un **10%** del parque Windows XP que tienen actualmente.

Principales razones para la renovación de software

En el ámbito industrial prevalece la continuidad del negocio, por lo que garantizar la producción es casi en el 50% de los casos la principal razón para la renovación del software industrial. Como hemos comentado ya, los fabricantes industriales establecen requisitos y condiciones que deben ser cumplidos por el usuario de los sistemas dentro del mantenimiento contratado, entre los que se suelen encontrar aspectos relativos a la actualización del software.

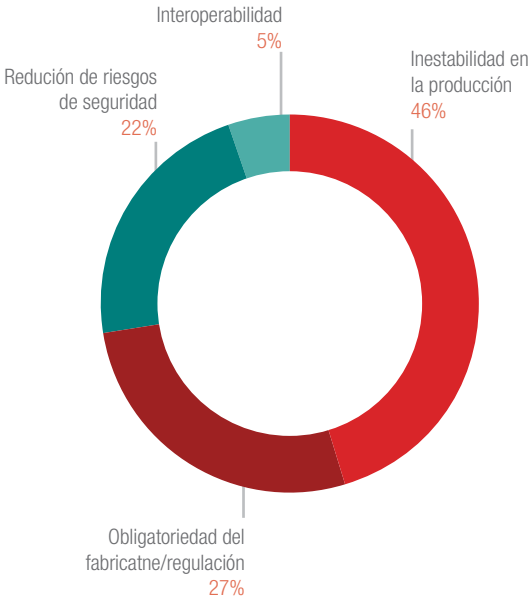


Ilustración 10 - Impulsores para la actualización.

Principales dificultades para migrar software en un entorno industrial

Como puede apreciarse en la gráfica la continuidad del proceso vuelve a ser el principal aspecto que determina la migración del software, seguido del elevado coste que supone actualizar el software en un entorno industrial.

Ilustración 11 - Inhibidores para la actualización.

3

Gestión de cambios y parches

Existe un gran desafío cuando se quiere implementar un programa de gestión de parches en los sistemas de automatización y control, especialmente con los propietarios de activos. Los cambios en el software industrial pueden afectar negativamente a su seguridad, operatividad y fiabilidad si no se realizan correctamente.

La gestión de parches en un entorno de automatización industrial requiere de gran cantidad de trabajo, especialmente para los propietarios de los activos, que para cada parche y para cada producto de su propiedad , tendrá que reunir y analizar información sobre cada dispositivo que posee, instalar y verificar todo en un sistema de prueba, realizar copias de seguridad antes y después , asegurar las pruebas y antes de apagar el sistema dar respaldo a las operaciones , y por último realizar el seguimiento de toda la documentación necesaria para realizar los cambios.

Debido a los recursos y al esfuerzo que se requiere para reparar un sistema de automatización de procesos, la mayoría de las organizaciones programan la aplicación de parches en paradas de mantenimiento rutinarias. Sin embargo, en ocasiones, estos lapsos de interrupción son trimestrales, anuales o incluso de más tiempo.

Algunos sistemas extremadamente críticos pueden no permitir lapsos de interrupción, y pueden, por tanto, no ser parcheados. La aplicación de parches debe estar contemplado dentro de la gestión de riesgos. Si el costo de la parada para aplicar los parches es mayor que el costo del riesgo evaluado , el parche debe ser aplazado, especialmente si hay otros controles de seguridad compensatorios en su lugar que mitiguen el riesgo.

Algunas consecuencias no deseadas de una gestión de parches errónea:

- Interferencia con la información de licencia de software.
- Incompatibilidad entre parches y el software del sistema de control.
- Virus y falsos positivos anti-malware.
- Degradación del rendimiento del sistema , de su confiabilidad y operatividad.

4

Impacto para el negocio

El principal impacto del software industrial sin soporte o sin una gestión adecuada de parches es su alto riesgo de pérdida de servicio o el compromiso de su integridad. A diferencia de los sistemas en tiempo no real, cuando se comprometen estos sistemas puede tener consecuencias más allá de la pérdida de datos o el tiempo de inactividad del sistema. Un compromiso de un sistema de automatización o control industrial puede afectar además de a la seguridad del sistema, a la seguridad física de personal de operaciones, a la calidad de los productos producidos, a la seguridad de los productos elaborados, y en algunos casos al medio ambiente o a la seguridad nacional.

El tiempo de inactividad de un sistema de automatización o control en una organización puede ser muy costoso, así como puede serlo la perdida de transacciones o su alteración en sistemas críticos. La mayoría de los incidentes de ciberseguridad tienen como resultado un tiempo de inactividad, ya sea como resultado directo de un ataque en sí mismo o como parte necesaria de los esfuerzos de remediación. Algunos de estos incidentes de ciberseguridad han dejado los sistemas críticos del negocio durante varios días ocasionando perdidas que han afectado directamente a la cuenta de resultados poniendo en riesgo la viabilidad y continuidad del negocio.

Antes de efectuar la actualización del software para evitar impactos en el negocio debe evaluarse previamente el impacto para el negocio y realizar su programación en periodos en que tenga un impacto mínimo.

5

Recomendaciones. Buenas prácticas

La Agencia Europea para la Seguridad de la Información y las Redes (ENISA) recomienda que para evitar la propagación de este tipo de incidentes es necesario:

- Los fabricantes deben adherirse al paradigma de la "seguridad desde el diseño" (security by design) y utilizar metodologías de seguridad en el ciclo de vida del software.
- CERTs que permitan identificar y clasificar las vulnerabilidades y los patrones de ataque, así como definir medidas compensatorias.
- La vigilancia de los usuarios , es decir, la concienciación y formación debe permitir al usuario detectar un comportamiento anormal de su sistema, permitir la detección rápida de la amenaza, instalar rápidamente parches publicados y seguir las pautas de configuración segura.

El CCN-CERT (Equipo de respuesta ante incidentes del Centro Criptológico Nacional) recomienda la elaboración de un plan de migración del parque de equipos con sistema operativo Windows XP a versiones más actualizadas a la mayor brevedad posible para reducir en la medida de lo posible el impacto de ausencia de soporte.

RECOMENDACIÓN PRACTICA

1. Elaborar un inventario de equipos cuyo sistema operativo esté próximo la finalización de su soporte, así como identificar su versión actual, ubicación, direccionamiento y conexión a red.

2. Clasificar los equipos existentes en base a la criticidad del proceso de negocio que soporta y al que puede afectar, estableciendo una prioridad de actuación en base a su importancia.

3. Identificar las aplicaciones que se están ejecutando en los sistemas, así como los proveedores del software, instalación y mantenimiento.

4. Contactar con cada uno de los proveedores para conocer su estrategia de actualización y herramientas recomendables para facilitar la preparación y actualización.

5. Realizar un análisis de riesgos de las distintas alternativas con la información recopilada.

6. Establecer un plan de actualización en aquellos sistemas que sea posible llevar a cabo la operación de actualización teniendo en cuenta:

a. Condiciones de fabricante en cuanto a coste y soporte.
b. La clasificación de criticidad para el negocio de cada sistema.
c. Los riesgos de actualizar el software.
d. Plan de Rollback.

7. Para aquellos equipos cuya actualización aún no es posible, analizar la implementación de medidas compensatorias que permitan mitigar el riesgo expuesto en este documento.

8. Establecer un periodo de verificación y seguimiento del comportamiento después de realizar los cambios.

La recomendación más importante en un entorno crítico, como es un proceso productivo, pasa por garantizar mediante SLAs o requisitos contractuales, que el fabricante de software evolucione su producto para soportar las versiones de tecnología del software base, como es el sistema operativo.

6

Conclusiones

En el entorno industrial un mal funcionamiento del software no solamente afectará a la funcionalidad, sino que tiene impactos e implicaciones mayores, pudiendo incluso desencadenarse una catástrofe.

El software que se comercializa como producto tiene que evolucionar a la vez que el entorno, no debe ser algo estático, sino que debe evolucionar hacia un servicio donde se establezcan SLAs adaptados a la criticidad de los sistemas.

Es importante lograr concienciar a los distintos actores involucrados, donde el fabricante, la ingeniería, el integrador y el usuario final tendrán que colaborar para disponer de un software “resilente”, necesario en el actual entorno de conectividad.

La previsión y el establecimiento de un procedimiento adecuado, como se describe en las recomendaciones, que permita mitigar el riesgo en un proceso ya automatizado, pero también en los proyectos nuevos debe contemplarse desde el principio un plan de actuación para cuando finalice el soporte del software.

La inacción no es una opción, debe planificarse la actualización del software o mitigar de alguna manera los riesgos residuales.

7

Recursos

- **Window of Exposure a real problem for SCADA**
  www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/window-of-exposure-a-real-problem-for-scada-systems
- **Microsoft Security Development Lifecycle**
  www.microsoft.com/security/sdl/default.aspx
- **Informe Gartner Creating a Timeline for Deploying Windows 7 and Eliminating Windows XP**
  www.gartner.com/newsroom/id/1378413
- **Microsoft Security Development Lifecycle**
  es.wikipedia.org/wiki/Microsoft_Windows
- **CLASP**
  www8.hp.com/us/en/software-solutions/software-security/index.html
- **OpenSAMM**
  www.opensamm.org
- **Microsoft Security Development Lifecycle**
  www.microsoft.com/security/sdl/default.aspx
- **Microsoft_Security_Intelligence_Report**
  www.microsoft.com/security/sir/
- **SDL Threat Modeling**
  www.microsoft.com/downloads/en/details.aspx?FamilyID=a48cccb1-814b-47b6-9d17-1e273f65ae19&displaylang=en
- **Sistemas operativos de tiempo real**
  es.wikipedia.org/wiki/Sistema_operativo_de_tiempo_real
- **Mitigating Risk. Why Sticking with Windows XP Is a Bad Idea (IDC)**
  www.microsoft.com/es-es/download/details.aspx?id=29883
- **Seguridad IT: invertir o convencer para invertir he ahí el dilema 1 de 3**
  www.bsecure.com.mx/featured/adrianpalma/
- **Riesgos de uso de Windows XP tras el fin de soporte**
  www.ccn-cert.cni.es/publico/dmpublidocuments/CCN-CERT_IA-02-14.pdf
- **Soporte Siemens**
  support.automation.siemens.com
- **Lifecycle Solutions & Servicies. Honeywell**
  www.honeywellprocess.com/library/marketing/notes/Experion-R410-Migration-XP-EOL-Service-Note.pdf
- **Windows XP End of Life. What it means for OSIsoft and the PI System**
  cdn.osisoft.com/corp/en/docs/misc/Windows%20XP%20Migration%20and%20The%20PI%20System.pdf
- **National Vulnerability Database**
  nvd.nist.gov
- **ISA - dTR62443 - 2 - 3 Security for industrial automation and control systems – Patch management in the IACS environment**
  http://isa99.isa.org/Documents/Drafts/ISA-TR62443-2-3-WD.pdf
- **Windows 8 - Centro de Compatibilidad**
  www.microsoft.com/en-us/Windows/compatibility/CompatCenter/Home?Language=en-US
- **Windows 8 - Asistente para actualización**
  Windows.microsoft.com/es-es/Windows-8/upgrade-assistant-advisor
- **Windows Assesment and Deployment Toolkit (ADK)**
  www.microsoft.com/es-es/download/details.aspx?id=30652
- **Microsoft Application Compatibility Tookit 5.6**
- www.microsoft.com/en-us/download/details.aspx?id=7352
- **Office 2013 Compatibility Guide**
  technet.microsoft.com/en-us/library/ee819096.aspx
- **Plan Impulso Pymes de Microsoft para actualización de XP**
  www.microsoft.com/business/es-es/catalogo-pymes/Paginas/fin-xp-y-office-2003.aspx
- **Fin de Soporte de XP: Microsoft**
  www.microsoft.com/es-es/windows/business/retiring-xp.aspx
- **Centro de Ciberseguridad Industrial**
  www.cci-es.org

C/ Maiquez, 18 · 28009 MADRID
Tel.: +34 910 910 751
e-mail: info@cci-es.org
www.cci-es.org
Blog: blog.cci-es.org
Twitter: @info_cci