Actualizaciones de software

Políticas de seguridad para la pyme

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. ACTUALIZACIONES DE SOFTWARE

1.1. Antecedentes

Todo software es susceptible de necesitar actualizaciones por motivos de seguridad, esto incluye el *firmware* de los equipos electrónicos, los sistemas operativos y aplicaciones informáticas e incluso los propios programas antimalware. Los fabricantes de software lanzan **actualizaciones** y **parches** que mejoran y añaden nuevas funcionalidades, o que corrigen errores y agujeros de seguridad.

Si no mantenemos **convenientemente actualizados** [1] nuestros equipos y aplicaciones nos exponemos a todo tipo de **riesgos** [2]**.** Los sistemas no actualizados son aprovechados por los delincuentes para introducirse en ellos y dejarlos inactivos, **infectarlos** (con lo que serían menos eficientes), aprovechar su capacidad de proceso para crear **botnets** con fines delictivos [3] y **robar** todo tipo de datos (credenciales de acceso, datos confidenciales, etc.).

Debemos ser conscientes sobre la necesidad de mantener permanentemente actualizado y parcheado todo nuestro software [4]. Tendremos en cuenta que existen aplicaciones que incluyen sistemas de **actualizaciones automáticas** que es recomendable aplicar. En los casos de actualización manual tendremos muy en cuenta que las fuentes de dónde obtenemos el software sean de confianza. En los casos en lo que tengamos servicios subcontratados a terceros, también exigiremos que el software este convenientemente actualizado.

Todo el software tiene un **ciclo de vida**, por lo que llegado el momento puede quedar **obsoleto** y sin soporte oficial por parte del fabricante. En ese momento es un blanco fácil para los ciberdelincuentes (sobre todo si estamos conectados a internet) y deberíamos dejar de utilizarlo.

1.2. Objetivos

Revisar la existencia de **actualizaciones** y **parches** de seguridad para nuestro software y elaborar procedimientos que permitan que tales actualizaciones y parches sean instalados en nuestros equipos de forma **segura** y **controlada**.

1.3. Checklist

A continuación se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a **actualizaciones de software**.

Los controles se clasificarán en dos niveles de **complejidad**:

- Básico (**B**): el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.
- Avanzado (**A**): el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente **alcance**:

- Procesos (**PRO**): aplica a la dirección o al personal de gestión.
- Tecnología (**TEC**): aplica al personal técnico especializado.
- Personas (**PER**): aplica a todo el personal.

NIVEL	ALCANCE	CONTROL	
B	PRO	**Determinar el software qué debe ser actualizado** Realizas un listado del software existente en la empresa para incluirlo en el plan de actualizaciones.	☐
B	TEC	**Determinar cuándo y qué actualizaciones instalar** Revisas las características y los requisitos de las actualizaciones y parches antes de instalarlos.	☐
A	TEC	**Probar las actualizaciones** Analizas y contrastas en un entorno de pruebas las actualizaciones que deseas instalar.	☐
A	TEC	**Deshacer los cambios** Cuentas con mecanismos y procedimientos para deshacer los cambios sufridos tras ejecutar una actualización en caso de no resultar conveniente.	☐
A	TEC	**Herramientas de diagnóstico y actualización** Utilizas herramientas de autodiagnóstico para detectar software no actualizado en tus equipos.	☐
B	TEC	**Configuración de un sistema de alertas** Tienes configurado un sistema de alertas para recibir avisos y notificaciones sobre vulnerabilidades, actualizaciones y parches de seguridad.	☐
B	TEC	**Registro de actualizaciones** Registras cada una de las actualizaciones y parches que instalas.	☐

Revisado por: _____ **Fecha:** _____

1.4. Puntos clave

Los puntos clave de esta política son:

- **Determinar el software qué debe ser actualizado.** Tendremos que realizar un inventario de todo el software y el *firmware* instalado, ya que pueden descubrirse errores o mejoras de funcionalidad. Para corregir dichos errores y garantizar un comportamiento óptimo debemos instalar, en cuando tengamos conocimiento de ellos, las correspondientes actualizaciones y parches de seguridad [4].
- **Determinar cuándo y qué actualizaciones instalar.** El equipo técnico determinará el momento en que ejecutar las actualizaciones para no interferir con las operaciones de la empresa. Aunque los principales programas comerciales disponen de funcionalidades de actualización automática, cabe la posibilidad de que tengamos software instalado que no disponga de estas opciones de actualización. En este caso usaremos los canales de alerta y los procedimientos oportunos para detectar e instalar las actualizaciones correspondientes. Antes de su instalación consideraremos la utilidad de las nuevas mejoras y la gravedad los errores que subsanan, así como los requisitos hardware/software necesarios.
- **Probar las actualizaciones.** Siempre debemos instalar actualizaciones provenientes de fuentes confiables. No obstante, se debe sopesar la necesidad de disponer de un entorno de pruebas o preproducción donde instalar y probar las actualizaciones, de este modo podremos verificar que su funcionamiento es el esperado. Es obligatorio realizarlo así en las actualizaciones de aplicaciones críticas instaladas en servidores (CMS, servidores web, servidores de correo, etc.).
- **Deshacer los cambios.** Antes de aceptar la instalación de una actualización, se debe considerar la forma de deshacer los cambios realizados. Así si el comportamiento del software actualizado no responde a lo esperado podremos volver a la situación anterior. Siempre es recomendable disponer antes de cualquier cambio de copias de seguridad recientes localizadas y probadas.
- **Herramientas de diagnóstico y actualización.** Existen herramientas que revisan si el software de nuestros equipos está actualizado o no. Una vez detectadas las actualizaciones pendientes, podemos proceder a su instalación en todos los equipos de manera centralizada. Esto puede ser útil en entornos con muchos equipos en los que queremos que el software instalado sea homogéneo y esté especialmente controlado.
- **Configuración de un sistema de alertas.** Conviene configurar un sistema de alertas para recopilar avisos [5] y notificaciones sobre vulnerabilidades, actualizaciones y parches de seguridad del software utilizado. Estas alertas pueden ser de varios tipos:
    - suscripciones a boletines genéricos sobre avisos y vulnerabilidades en la red [6] [7];
    - suscripciones a boletines específicos sobre actualizaciones y novedades acerca de los productos y servicios software que utilizamos;
    - seguimiento en redes sociales de las publicaciones especializadas en ciberseguridad;
    - revisión periódica de medios y fuentes especializados;
    - configuración de sistemas de avisos RSS [8].
- **Registro de actualizaciones.** Realizaremos un registro de las actualizaciones que se han instalado en nuestros sistemas. De esta forma podremos tener en todo momento un conocimiento exhaustivo del software operativo en nuestros equipos.

2. REFERENCIAS

[1]. Incibe – Protege tu empresa – Blog – Si tu pyme protegida quiere estar, siempre tienes que actualizar (infografía) https://www.incibe.es/protege-tu-empresa/blog/si-tu-pyme-protegida-quiere-estar-siempre-tienes-actualizar

[2]. ENISA – Threat Landscape Report 2017 (en) https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

[3]. OSI – Qué es una botnet o una red zombi de ordenadores https://www.osi.es/actualidad/blog/2014/03/14/que-es-una-botnet-o-una-red-zombi-de-ordenadores

[4]. OSI – La importancia de las actualizaciones de seguridad https://www.osi.es/es/actualizaciones-de-seguridad

[5]. Incibe – Protege tu empresa – Avisos de seguridad https://www.incibe.es/protege-tu-empresa/avisos-seguridad

[6]. Incibe – Boletines de seguridad https://www.incibe.es/suscripciones

[7]. CERTSI – Suscripción a boletines de CERTSI https://www.certsi.es/suscripciones

[8]. Incibe – Avisos de Seguridad RSS https://www.incibe.es/feed/avisos-seguridad/all

[9]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Uso de dispositivos móviles corporativos https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[10]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Protección del puesto de trabajo https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[11]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Uso de dispositivos móviles no corporativos https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[12]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Aplicaciones permitidas https://www.incibe.es/protege-tu-empresa/herramientas/politicas

INSTITUTO NACIONAL DE CIBERSEGURIDAD