Antimalware

Políticas de seguridad para la pyme

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. ANTIMALWARE

1.1. Antecedentes

La aparición constante de nuevos **virus** y otros tipos de **malware** [1] es una de las principales **amenazas** a las que se enfrentan hoy en día nuestros sistemas.

Las vías de contagio por malware son numerosas, destacando entre otras:

- las descargas de ficheros de todo tipo, adjuntos en correos o desde páginas web;
- la navegación por webs de dudosa fiabilidad;
- y la utilización de dispositivos ajenos, por ejemplo pendrives.

El enorme daño que pueden causar a nuestra organización hace obligatorio el establecimiento de una **política de control de malware**. De este modo podremos prevenir, detectar, controlar y eliminar la ejecución de cualquier software malicioso en nuestros sistemas.

1.2. Objetivos

Proteger todos los activos de información de la empresa contra la infección por **virus** o cualquier otro tipo de **malware**.

1.3. Checklist

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

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	**Instalar o contratar una solución antimalware** Analizas en detalle qué tipo de solución antimalware es la más apropiada para tu empresa y la contratas o la instalas.	☐
A	TEC	**Configurar las herramientas de detección de malware** Configuras correctamente todas las funcionalidades de tus herramientas de control de malware.	☐
B	TEC	**Actualizar las herramientas de detección de malware** Actualizas cada _____ las herramientas de detección y control de malware que tienes instaladas.	☐
A	TEC	**Establecer el procedimiento de respuesta ante la infección por ejecución de malware** Elaboras procedimientos detallados de actuación ante infecciones por malware.	☐
B	PER	**Buenas prácticas para el control de malware** Sigues las directrices básicas para prevenir las infecciones por malware.	☐

Revisado por: _____ **Fecha:** _____

1.4. Puntos clave

Los puntos clave de esta política son:

- **Determinar qué tipo de soluciones serán las más convenientes para nuestra empresa.** Dependiendo del tamaño [2] de nuestra organización, del nivel de seguridad necesario y de la complejidad de las configuraciones [3] para la protección de nuestros activos de información, podremos determinar distintos tipos de soluciones:
  - herramientas para el puesto de trabajo, el portátil o los dispositivos móviles,
  - soluciones globales corporativas entre ellas:
    - UTM o gestión unificada de amenazas;
    - servicios gestionados que nos pueden facilitar nuestros proveedores de servicios de internet (ISP) u otros proveedores desde un centro de operaciones de seguridad o SOC;
    - soluciones de seguridad ofrecidas como servicios en la nube que monitorizan nuestros equipos de forma remota.

  Para el tipo de solución elegida, seleccionaremos la más apropiada de entre las disponibles en el mercado [4] buscando la compatibilidad con nuestras infraestructuras y la versatilidad (antimalware, antiphishing, antispam, análisis de web y correo,…) de la herramienta.
- **Configurar las herramientas de detección de malware.** Para un uso eficiente de las herramientas de control de malware se debe realizar una correcta configuración de todas sus funcionalidades. La configuración deberá permitirnos, entre otros, establecer los siguientes controles:
  - realizar análisis automáticos y periódicos para detectar malware;
  - realizar comprobaciones automáticas de los ficheros adjuntos al correo y de las descargas web, ya que pueden contener código malicioso ejecutable;
  - bloquear el acceso a ciertas aplicaciones o sitios web basándonos en una política de listas negras;
  - permitir el acceso a ciertas aplicaciones o sitios web basándonos en una política de listas blancas;
  - permitir el análisis de páginas web para detectar posibles amenazas incluidas en las mismas.
- **Actualizar las herramientas de detección de malware.** Debemos determinar la periodicidad con la que las herramientas de detección de malware son actualizadas. Actualmente se crean miles de virus al día, por lo que las actualizaciones de la base de datos de firmas de virus deberían ser automáticas y tener una periodicidad como mínimo diaria. Por otro lado, y como cualquier otra aplicación crítica, tendremos que actualizar convenientemente el propio software antivirus [6].
- **Establecer el procedimiento de respuesta ante la infección por ejecución de malware.** En primer lugar determinaremos qué sucesos serán considerados como incidencias por ejecución de malware, analizando:
  - el impacto del ataque;
  - los activos que puedan estar comprometidos;
  - la forma de recuperar los activos impactados;
  - los canales adecuados de aviso y notificación.

Después estableceremos las responsabilidades y la operativa a seguir en cada caso:

- desinfección de ficheros;
- eliminación de ficheros;
- aviso a soporte técnico del fabricante;
- reinstalación de software afectado;
- desconexión y asilamiento del equipo afectado;
- y el registro formal del incidente.

- **Política general de buenas prácticas para el control de malware.** Con el fin de reforzar las medidas establecidas para el control del malware es conveniente tener concienciada a la plantilla en los siguientes aspectos:
  - Se deben considerar todos los contenidos y las descargas como potencialmente inseguros hasta que no sean convenientemente analizados por una herramienta de detección de malware.
  - Deben prohibirse las siguientes acciones:
    - Ejecutar ficheros descargados de servidores externos, de soportes móviles no controlados o adjuntos a correos, sin haber sido previamente analizados.
    - Configurar el programa cliente de correo electrónico para la ejecución automática de contenido recibido por correo.
    - Alterar la configuración de seguridad establecida para los sistemas y equipos de tratamiento de información.
  - Debe utilizarse únicamente el software permitido [7] por la organización. Este además debe estar convenientemente actualizado [6].
  - Para evitar la recepción de spam se deben seguir las directrices incluidas en la política de correo electrónico [8].

2. REFERENCIAS

[1]. Incibe – Protege tu empresa – Blog – Descubre los diferentes tipos de malware que pueden afectar a tu pyme https://www.incibe.es/protege-tu-empresa/blog/descubre-tipos-malware

[2]. Incibe – Protege tu empresa – Blog – Descubre cómo proteger tu empresa del malware https://www.incibe.es/protege-tu-empresa/blog/descubre-proteger-tu-empresa-del-malware

[3]. Incibe – Protege tu empresa – Blog – 10 armas del gladiador antimalware https://www.incibe.es/protege-tu-empresa/blog/10-armas-del-gladiador-antimalware

[4]. Incibe – Protege tu empresa – Herramientas – Catálogo de empresas y soluciones de ciberseguridad https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad

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

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

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

[8]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Uso de correo electrónico https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[9]. 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

[10]. 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

[11]. 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

INSTITUTO NACIONAL DE CIBERSEGURIDAD