Ciberseguridad Avanzada

MEDIDAS DE PROTECCIÓN ANTI RANSOMWARE

Inycom
innovation technologies

Tras la virulencia y extensión del ataque global de Wannacry se hace necesario reforzar aún más si cabe las medidas de protección de nuestros sistemas para proteger tanto a nuestras compañías como a los servicios públicos esenciales.

Desde el departamento de Consultoría de Seguridad y Operaciones hemos preparado una guía con las principales medidas de protección y recuperación ante ataques como Wannacry y otros Ransomware que nos van a afectar durante las próximas semanas y meses.

Estas son las medidas que proponemos a nuestros clientes y que aplicamos desde nuestra Area de Servicios de Infraestructuras.

www.inycom.es

trends.inycom.es

INSTALACIÓN DE HERRAMIENTAS ANTI-RANSOMWARE

Desde Inycom recomendamos la implantación de herramientas Anti-Ransomware en todos los equipos.

Este tipo de herramientas están basados en el estudio de comportamientos anómalos del puesto de trabajo y bloquean los procesos de cifrado de disco en el mismo momento de producirse. Adicionalmente bloquean también el acceso a zonas de memoria restringidas y evitan el escalado de privilegios en los equipos.

Son las soluciones que se han demostrado más eficaces en la protección de equipos, tanto de TIC como de equipos Industriales.

UTILIZACIÓN DE ENTORNOS VIRTUALIZADOS PARA EL PUESTO DE TRABAJO Y MICROSEGMENTACIÓN DE SERVIDORES

En este ataque se ha comprobado que las empresas con entornos de escritorio virtualizados (VDI) han sido menos afectados por la infección.

Esto ha sido debido a varias ventajas de este tipo de entornos:

- Son más fáciles de mantener y actualizar (se gestiona una sola imagen)
- Permiten aislar los equipos de los distintos departamentos
- Permiten la microsegmentación y protección de servidores que los mantienen aislados de las redes afectadas.

CONCIENCIACIÓN SOBRE LA IMPORTANCIA DE LA CIBERSEGURIDAD

Esta recomendación, aunque esté en último lugar es la más importante.

Es fundamental que la dirección de la compañía, los responsables de la toma de decisiones y los trabajadores de la información seamos conscientes de los peligros provocados por los Cibercriminales y tengamos en cuenta estos peligros en nuestro trabajo diario y en la relación con el resto de usuarios.

COPIAS DE SEGURIDAD ACTUALIZADAS Y AISLADAS DEL ENTORNO DE PRODUCCIÓN

Recomendamos mantener copias de seguridad de los datos críticos que nos permitan recuperar la información con al menos 3-5 días de profundidad.

En este sentido recomendamos los servicios de Backup en Cloud que nos permiten un archivado de backup muy efectivo, a bajo coste y asilado de las unidades de red que suelen ser encriptadas por los Ransomware.

ACTUALIZACIÓN CONTINUA DE PARCHES DE SEGURIDAD

Es importante contar son sistemas automatizados que distribuyan diariamente los últimos parches de seguridad publicados, tanto pata los sistemas operativos como para las aplicaciones y navegadores utilizados por los usuarios.

Recomendamos la implantación o revisión de sistemas como WSUS, System Center, GPO u otros sistemas de distribución de Software corporativos

MANTENER NUESTROS SISTEMAS DE ANTIVIRUS ACTUALIZADOS

Hemos detectado en varias instalaciones que, aunque las firmas de antivirus suelen estar actualizadas, nos suele ocurrir lo mismo con las consolas de gestión y los agentes locales instalados en los Pc. Un comportamiento habitual en este tipo de ataques con virus tipo "gusano" es que lo primero que intenten es parar los antivirus instalados en los Pc para luego infectar los equipos

IMPLANTAR SISTEMAS DE ANTISPAM AVANZADOS

El correo electrónico es una de las puertas de entrada más habitual para los Ransomware. Contamos con soluciones de Antispam avanzado que utilizan tecnologías de Sansboxing (análisis Cloud en entornos aislados).

En concreto las soluciones de Advanced Threat Protection, analizan el comportamiento de ficheros adjuntos maliciosos y links en el correo.

REFORZAR POLÍTICAS GPO DE EJECUCIÓN DE APLICACIONES

Es necesario definir políticas de seguridad que eviten la ejecución de aplicaciones desde directorios habitualmente utilizados por los Ransomware (App Data\Local , Roaming) y bloquear la ejecución de archivos con extensiones "peligrosas".

EVITAR EN LOS EQUIPOS EL USO CUENTAS CON PRIVILEGIOS DE ADMINISTRADOR

En las distintas fases de un ataque, justo después de la infección inicial, el virus intenta un escalado de privilegios y un "movimiento lateral" hacia otros equipos de la red.

Si la cuenta del equipo infectado tiene permisos de administrador , esto va a facilitar la propagación de la infección por toda nuestra red.

Confiamos en que estas medidas permitan mantener la disponibilidad de sus sistemas y esperamos poder asesorarles sobre las Soluciones y Servicios de Ciberseguridad que ofrecemos desde INYCOM.

+34 902 995 820
info@inycom.es