PRIMER ENTREGABLE
CONTROL 8: MALWARE DEFENSE

JOSE ALEJANDRO MONTOYA GONZALEZ
LUIS FERNANDO CARDONA GALLEGO

PROFESOR
JUAN GABRIEL OSSA

UNIVERSIDAD DE MEDELLÍN
FACULTAD DE INGENIERÍA
INGENIERÍA DE SISTEMAS
MEDELLÍN
2020

¿EN QUÉ CONSISTE EL CONTROL?

El control de defensa contra el software malicioso (malware defense en inglés) se encarga de controlar la instalación, propagación y ejecución de software potencialmente dañino, se apoya en la automatización para mejorar la respuesta y actualización de la defensa además de recopilar datos para facilitar acciones correctivas

¿POR QUÉ ES IMPORTANTE ESTE CONTROL?

Debido a que el software malicioso (malware en inglés) es un aspecto integral y peligroso de las amenazas en internet, ya que está diseñado para atacar los sistemas, dispositivos y sus datos. Se propaga y cambia rápidamente, entra a través de múltiples y diversos puntos, como dispositivos de usuario final, archivos adjuntos de correo electrónico, medio extraíbles, servicios en la nube, entre otros. El malware moderno está diseñado para evitar las defensas, atacarlas o deshabilitar.

Por esta razón las herramientas contra el malware deben responder deben ser bastante versátiles, fáciles de escalar, fáciles de integrar con los demás procesos de seguridad. Además de que es necesario implementarlas en todos los puntos propensos a ataques.

¿CON CUÁLES CONTROLES SE RELACIONA?

Este control se encuentra relacionado en menor o mayor medida con todos los controles ya que cualquier interacción física o digital con el sistema es candidata a ser una punto de entrada para una infección de código malicioso. Se podría decir que este control en el aspecto técnico es la columna vertebral de la seguridad cibernética. Por esta razón listamos los controles en los que consideramos que esta relación es más crítica

- Control 1: Inventario de dispositivos autorizados y no autorizados.
- Control 2: Inventario de software autorizados y no autorizados.
- Control 3: Gestión continua de vulnerabilidades.

- Control 4: Uso controlado de privilegios administrativos.
- Control 5: Configuración segura para hardware y software en dispositivos. móviles, computadoras portátiles, estaciones de trabajo y servidores.
- Control 6: Mantenimiento, monitoreo y análisis de logs de auditoría.
- Control 7: Protección de correo electrónico y navegador web.
- Control 12: Defensa de borde.

¿CÓMO SE RELACIONA CON ESTOS CONTROLES Y EL POR QUÉ DE SU RELACIÓN?

El control

¿CÓMO, AL APLICAR EL CONTROL, SE MEJORA LA SEGURIDAD?

Mejora de forma bastante notoria ya que después de que un ataque traspase las barreras de borde como los firewall este control sería el encargado de detectar, detener y tomar las acciones necesarias para que el ataque sea infructuoso o en su defecto reducir lo más posible los daños. Otra ventaja es la retroalimentación que se puede obtener luego de que ocurre un incidente, esta información se puede usar para pulir las falencias del sistema propio además de servir como apoyo para que terceros pulan las de ellos antes de que sufran un ataque.

HERRAMIENTA

Nombre: ClamAV

Licencia: General Public License 2 (Licencia pública general)

La cual permite que cada usuario modifique el código fuente y publique nuevas versiones.

REQUISITOS DEL SISTEMA RECOMENDADOS:

RAM mínima recomendada:

Edición de servidor FreeBSD y Linux: 1 GiB +
Edición sin servidor Linux: 2 GiB +
Windows 7 y 10 de 32 bits: 2 GiB +
Windows 7 y 10 de 64 bits: 3 GiB +
macOS: 3 GiB +

CPU mínima recomendada:

Sistemas FreeBSD y Linux: 1 CPU 2.0 Ghz +
Windows 7 y 10: 1 CPU 2.0 Ghz +
OSX: 2 CPU a 2.0 Ghz +
Espacio mínimo disponible en el disco duro requerido:

Para la aplicación ClamAV, recomendamos tener 5 GB de espacio libre disponible. Esta recomendación es adicional al espacio en disco recomendado para cada sistema operativo.

Tenga en cuenta : Las pruebas para determinar estos requisitos mínimos se realizaron en sistemas que no ejecutaban otras aplicaciones. Si se ejecutan otras aplicaciones en el sistema, se requerirán recursos adicionales además de nuestros mínimos recomendados.

BIBLIOGRAFIA

https://www.clamav.net/documents/introduction

https://www.clamav.net/documents/clam-antivirus-user-manual

https://www.gnu.org/licenses/old-licenses/gpl-2.0-faq.es.html

https://gitlab.com/udem1/ciberseguridad/-/blob/master/documents/CIS-Controls-Version-7-Spanish.pdf

VS

https://securityaffairs.co/wordpress/40739/malware/av-test-antivirus-linux.html

https://www.datanyze.com/market-share/ep--359/clamav-vs-mcafee-virusscan