WIRELESS ACCESS CONTROL

DIEGO ASSIA

JUAN CARMONA

CIS CONTROL

CIBERSEGURIDAD

UNIVERSIDAD DE MEDELLIN

TABLA DE CONTENIDO

¿EN QUE CONSISTE EL CONTROL?

EL control denominado control de acceso inalámbrico “Wireless Access Control” consiste en rastrear, controlar, prevenir y corregir el uso seguro de los diferentes sistemas inalámbricos (Access point, WLAN, entre otros).

¿POR QUÉ ES IMPORTANTE ESTE CONTROL?

En la actualidad se han presentado grandes robos de datos a organizaciones, gracias a que terceros de la compañía consiguen conectarse a las redes inalámbricas de estas, quienes logran burlar la seguridad básica del sistema pudiendo así extraer grandes cantidades de datos. También existe la posibilidad de robar información cuando se están conectados a redes públicas, las cuales pueden ser usadas por los hackers como camuflaje para acceder a los distintos dispositivos que se conecten a estas; todo esto es posible debido a la in-necesidad de estar conectado físicamente para tener acceso al tráfico de datos.

¿CON CUALES CONTROLES SE RELACIONA?

El control de acceso inalámbrico “Wireless Access Control” se relaciona con todos los controles, pero se tiene más afinidad con los siguientes ya que estos hacen parte de la conectividad a la red, trafico de datos y vulnerabilidades.

- Control 1: Inventario de Dispositivos autorizados y no autorizados
- Control 3: Gestión continua de vulnerabilidades
- Control 4: Uso controlado de privilegios administrativos
- Control 8: Defensa contra malware
- Control 9: Limitación y control de puertos de red, protocolos y servicios
- Control 11: Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores
- Control 12: Defensa de borde
- Control 13: Protección de datos
- Control 14: Control de acceso basado en la necesidad de conocer

- Control 20: Pruebas de penetración y ejercicios de equipo rojo

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

- Control 1: Inventario de Dispositivos autorizados y no autorizados

  Este control permite gestionar los dispositivos que se encuentran el la red de la organización y a los datos a los cuales pueden acceder estos. Así que si algún dispositivo logra vulnerar el control de acceso inalámbrico y acceder a la red de la empresa este control es quien se encarga de gestionar a que datos puede acceder.
- Control 3: Gestión continua de vulnerabilidades

  Al encargarse de gestionar las vulnerabilidades de a los atacantes, este control está en total capacidad de anticipar la posibilidad de que el control de acceso inalámbrico, ya que si este presenta fallas la Gestión Continua De Vulnerabilidades las detectará.
- Control 4: Uso controlado de privilegios administrativos

  El uso controlado de privilegios administrativos evita que aquellos terceros que se logren conectar a la red de la organización ejecuten acciones o cambios en la información o composición de la empresa que pueden acarrear grandes consecuencias.
- Control 8: Defensa contra malware

  En caso de una violación al control 15 es este quien se debe asegurar que el intruso instale, propague e implante código que provoque que las defensas de la organización se desactiven o se realice otra acción maliciosa.
- Control 9: Limitación y control de puertos de red, protocolos y servicios

  Este control es el que se encuentra relacionado de forma mas directa con el control 15, debido a que la existencia de puertos, protocolos y servicios con vulnerabilidad es una ventana de oro para que quienes consigan conectarse a la red de la organización realicen acciones maliciosas y/o consigan extraer información de carácter confidencial de la compañía.

- Control 11: Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores.

  Al encargarse de gestionar toda la información de seguridad de la infraestructura de red de la organización acá es donde se cierran las puertas traseras para cortar las opciones a quienes logren infiltrarse en la red.
- Control 13: Protección de datos

  Una correcta protección de los datos asegura a la organización que su legibilidad por parte de terceros, que logren acceder a la red, sea nula, así se asegura que en caso que se realice una filtración de datos estos no se puedan visualizar debido a los protocolos de encriptamiento.
- Control 14: Control de acceso basado en la necesidad de conocer

  Si bien el cifrado de datos proporciona seguridad ante aquellos que logren violar el protocolo 15, este control ayuda a disminuir la cantidad de información a la que los intrusos logran acceder sin que los administradores y/o usuarios del sistema lo noten.

¿CÓMO SE MEJORA LA SEGURIDAD AL IMPLEMENTAR EL CONTROL?

La implementación de este control trae beneficios que contribuyen al mejoramiento de la seguridad, tal como la implementación de los demás controles. Con el control actual garantizamos que el rango de acción de posibles ataques se ve reducido considerablemente ya que se limitan las tecnologías inalámbricas, las cuales son muy usadas en la sociedad actual. Adicionalmente, si complementamos el control actual con otros muy afines como “Limitación y control de puertos de red, protocolos y servicios” (control 9) se disminuye aun mas la probabilidad de éxito de quieran atacar la seguridad.

HERRAMIENTA APLICACIÓN DEL CONTROL

La herramienta open source elegida para la aplicación del control es “OPENNAC”.

LICENCIA

En la página oficial de Opennac nos mencionan que el software posee licencia OSLv3. Dicha licencia indica: “1) Concesión de licencia de copyright. El Licenciante le otorga una licencia mundial, libre de regalías, no exclusiva y sublicenciable, por la duración de los derechos de autor, para: reproducir la obra original en copias, ya sea solo o como parte de una obra colectiva; traducir, adaptar, alterar, transformar, modificar u organizar el Trabajo original, creando así trabajos derivados ("Trabajos derivados") basados en el Trabajo original. Para informacion más detallada de la licencia https://opensource.org/licenses/OSL-3.0

REQUERIMIENTOS TÉCNICOS

Sistema Operativo: Windows 10, Linux, Mac OS X

Ram: Al menos 4GB

Hard Disk: 40gb

Tarjeta de red

COMPARACIÓN HERRAMIENTA ELEGIDA CONTRA HERRAMIENTA DE PAGO

La herramienta de pago con tendremos en cuenta para realizar la comparación es “Manage Engine Open Manager”, la principal diferencia entre este software y el seleccionado por nosotros es la posibilidad de hacer un monitoreo a niveles más profundos sobre los dispositivos que se encuentra en la red.

En cuanto a la licencia de funcionamiento de esta, permite hacer uso de la herramienta (después de realizar la respectiva compra) de forma única, no permite realizar modificaciones al software o redistribuirlo; caso contrario al ofrecido por OPENNAC, que al ser Open Source nos da total libertad para realizar estas y mas acciones.

WEBGRAFÍA

- https://www.manageengine.com/network-monitoring/index2.html
  https://www.cisecurity.org/wp-content/uploads/2017/09/CIS-Controls-Guide-for-SMEs.pdf
- https://www.newnettechnologies.com/cis-control-15.html
- https://www.softwaretestinghelp.com/network-scanning-tools/
- https://angryip.org/download/#source
- https://www.portablefreeware.com/index.php?id=268
- https://www.cisecurity.org/controls/cis-controls-faq/