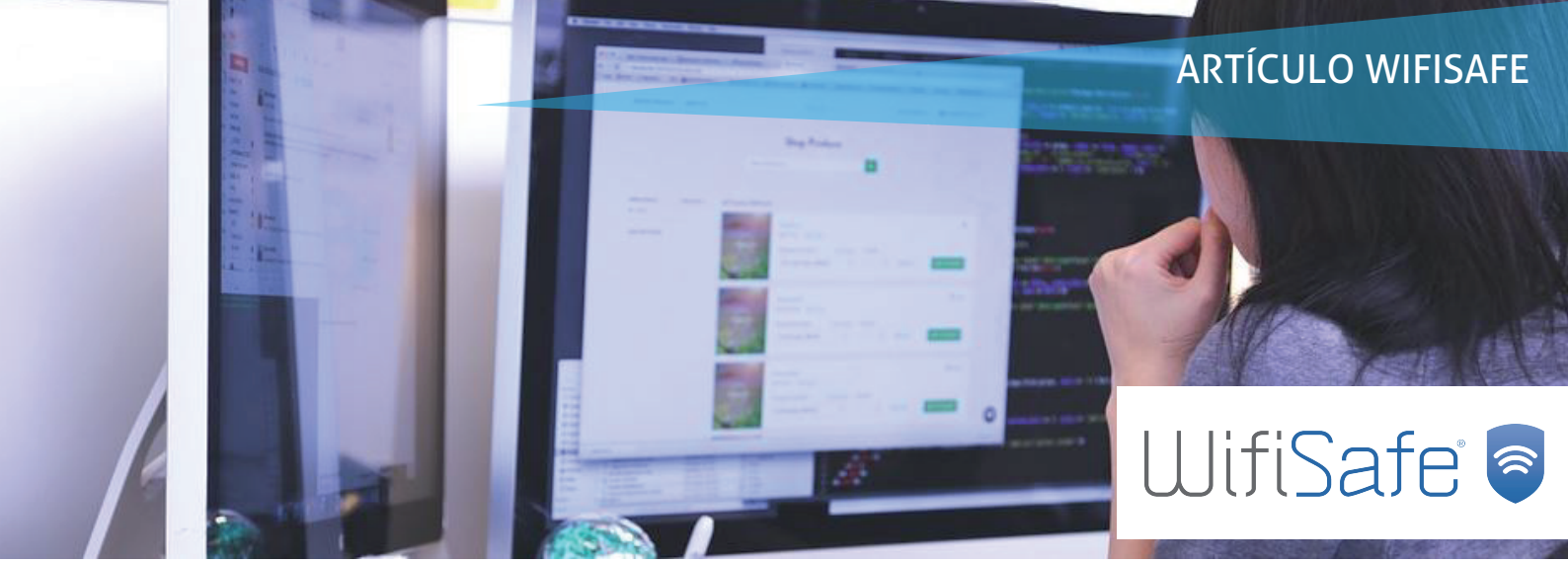

SEGURIDAD WIFI EN REDES EMPRESARIALES

2019 - WifiSafe

Material recomendado

- Blog | Manuales

Esta guía resume buenas prácticas y detalles técnicos para proteger las redes inalámbricas de amenazas y para implementar de manera segura, el acceso inalámbrico a las redes WiFi.

Nos centraremos específicamente en la tecnología inalámbricas "WiFi", ofreciendo recomendaciones generales que abordan las amenazas inalámbricas universales, para todas las redes y se describen controles de seguridad que pueden trabajarse para mitigar estas amenazas.

Las señales de WiFi pueden infiltrarse en los espacios de proveedores comerciales, edificios, negocios adyacentes y otros servicios disponibles públicamente.

Los servicios de WiFi públicos y privados, se pueden utilizar para obtener acceso no autorizado a redes que de otra manera, están fuertemente protegidas.

Debido a la naturaleza generalizada del WiFi, es importante considerar los riesgos asociados con estas tecnologías y examinar el posible impacto a la confidencialidad, disponibilidad e integridad, al realizar análisis de riesgos y amenazas.

Tipos de amenazas

La supervisión de la actividad y los dispositivos inalámbricos, permite a una empresa tener una mejor visibilidad del uso de WiFi e identificar y mitigar las amenazas relacionadas con el servicio.

Al no abordarse la seguridad inalámbrica, las redes empresariales están expuestas a las amenazas que se enumeran a continuación.

Las amenazas de WiFi incluyen:

- Puntos de acceso ocultos o dudosos (AP): los puntos de acceso inalámbricos no autorizados conectados a la red de la empresa, no pueden transmitir su identificador de conjunto de servicios (SSID) para ocultar su existencia.

- AP mal configurados: los AP's con configuraciones débiles o incorrectas que permiten que dispositivos no autorizados, se conecten o expongan las comunicaciones de conexión a ataques de sniff y repeticiones.

- Dispositivos prohibidos: dispositivos no permitidos en la red por la política de la organización (por ejemplo, dispositivos de almacenamiento inalámbrico).

- Clientes de asociación incorrecta: los clientes que utilizan redes no seguras y sin supervisión cuando las conexiones de red seguras y monitoreadas están disponibles, propiciando el riesgo de pérdida de datos y compromiso del sistema.

- Clientes no autorizados: clientes no autorizados que se conectan a la red. Los clientes malintencionados presentan riesgos de puente y pérdida de datos, así como eludir los controles de seguridad establecidos y los esfuerzos de monitoreo.

• Clientes de conexión compartida y puente de conexión a Internet: un dispositivo que comparte su conexión a Internet o permite la conectividad a múltiples redes al mismo tiempo, puede usarse para omitir la supervisión de la red y los controles de seguridad y puede provocar la pérdida de datos o proporcionar un punto de entrada de red no seguro para un atacante.

• Asociación no autorizada: una asociación de punto de acceso a punto de acceso que puede violar el perímetro de seguridad de la red.

• Conexiones Ad-Hoc: una conexión de red de igual a igual que puede violar el perímetro de seguridad de la red.

• AP de Honeypot / Evil Twin: una configuración de AP para hacerse pasar por puntos de acceso autorizados que interceptan las comunicaciones de red y comprometen los sistemas que se conectan a él.

• Ataques de denegación de servicio (DoS): un ataque que busca abrumar al sistema y ocasionar que falle o degrade su capacidad de uso.

Prevención de amenazas

Un sistema de prevención de intrusión inalámbrica activo , permite que las redes empresariales creen y apliquen políticas de seguridad inalámbrica.

¿Qué es un sistema de prevención de intrusión inalámbrica?

Un sistema de prevención de intrusión inalámbrica (conocido por sus siglas en inglés WIPS), es un hardware de red que supervisa el espectro radioeléctrico para detectar la presencia de puntos de acceso no autorizados (detección de intrusión) y para tomar contramedidas (prevención de intrusos) automáticamente.

El principal objetivo de un WIPS, es evitar el acceso no autorizado a una red de área local y otros activos de información mediante dispositivos inalámbricos.

Estos sistemas generalmente se implementan como una superposición a una infraestructura LAN inalámbrica existente, aunque pueden implementarse de manera independiente para aplicar políticas no inalámbricas dentro de una empresa.

Las grandes organizaciones con muchas empleados, son particularmente vulnerables a las brechas de seguridad causadas por puntos de acceso desautorizados.

Las configuraciones de WIPS constan de tres componentes:

> Sensores: estos dispositivos contienen antenas y radios que escanean el espectro inalámbrico en busca de paquetes y se instalan en todas las áreas a proteger.

> Servidor: el servidor WIPS analiza de forma centralizada los paquetes capturados por los sensores.

> Consola: la consola proporciona la interfaz de usuario principal en el sistema para la administración y la generación de informes.

Un sistema simple de detección de intrusos puede ser un solo ordenador, conectado a un dispositivo de procesamiento de señal inalámbrico, y antenas ubicadas en toda la instalación.

Un WIPS, proporciona la capacidad de monitorear y administrar de manera centralizada la seguridad inalámbrica de la empresa, con respecto a las diversas amenazas enumeradas anteriormente.

Alternativamente, durante un incidente relacionado con estas amenazas, se requeriría que un técnico en el lugar, encuestara a toda la empresa con un ordenador portátil u otro dispositivo de detección de red inalámbrica en un intento de localizar e identificar un acceso no autorizado.

Tener un sistema de prevención de intrusión inalámbrica, ayuda enormemente en la remediación de incidentes.

Identificar y mitigar con éxito los AP ilegales y los dispositivos inalámbricos que intervienen, es un proceso difícil y laborioso, ya que los puntos de acceso no autorizados, se mueven con frecuencia y no siempre se encienden.

Un sistema de prevención de intrusión inalámbrica proporciona alertas automáticas, inmediatas al centro de operaciones de seguridad empresarial y puede configurarse para evitar automáticamente que los clientes se conecten a puntos de acceso no autorizados.

Las sistema de prevención de intrusión inalámbrica también son útiles para localizar físicamente los puntos de acceso no autorizados para eliminarlos.

Requisitos recomendados para WIPS

Incluso las redes cableadas que no admiten el acceso inalámbrico deben utilizar una solución WIPS para monitorear y detectar puntos de acceso no autorizados y conexiones no autorizadas.

La siguiente lista incluye los requisitos específicos recomendados para las redes de sensores WIPS y debe adaptarse según las consideraciones locales y los requisitos de cumplimiento aplicables.

Los sistemas WIDS / WIPS deben incluir las siguientes características:

• Capacidad de detección de clientes maliciosos. El sistema detectará de manera confiable la presencia de una estación de trabajo que transmite simultáneamente IP desde una segunda tarjeta de interfaz de red inalámbrica (NIC).

• Tener una capacidad de detección WAP rogue. La capacidad de detección de WAP debe detectar de manera confiable la presencia de un WAP que se comunica dentro del perímetro físico de la empresa.

• Tener una capacidad de proceso de detección de intrusos. La detección de WAP o cliente no autorizado, se producirá independientemente de las técnicas de autenticación o cifrado que esté utilizando el dispositivo infractor (por ejemplo, traducción de direcciones de red (NAT), cifrado y WAP de software). La detección fraudulenta debe combinar técnicas por aire y por cable para exponer de manera confiable los dispositivos fraudulentos.

• Detecte y clasifique dispositivos móviles WiFi como iPads, iPods, iPhones, dispositivos Android, Nooks y MiFi.

• Detecte los dispositivos 802.11a/b/g/n/ac conectados a la red cableada o inalámbrica.

• Ser capaz de detectar y bloquear múltiples WAP desde un solo dispositivo sensor a través de múltiples canales inalámbricos.

• Ser capaz de imponer una política de "no WiFi" por subred y en múltiples subredes.

• Bloquee múltiples instancias simultáneas de lo siguiente: ataques DoS, conexiones Ad hoc, asociaciones incorrectas de clientes, falsificación de direcciones de control de acceso de medios (MAC), WAP de Honeypot, WAP malintencionados, WAP mal configurados y asociaciones no autorizadas.

• Detecte e informe ataques adicionales mientras bloquea las vulnerabilidades enumeradas anteriormente (las capacidades de detección e informe no se verán afectadas durante la prevención).

• No afecta a ningún dispositivo WiFi externo (vecino). Esto incluye intentar conectarse por aire para proporcionar huellas digitales en la Capa Dos; por lo tanto, el uso de tablas de memoria direccionable de contenido (CAM) existentes, no es aceptable para cumplir con este requisito.

• Proporcionar comunicaciones mínimas entre el sensor y el servidor, y se debe identificar un mínimo de Kbps permitido específico. El sistema proporcionará una clasificación automática de clientes y WAP según la política y de la empresa.

• Proporcionar comunicaciones seguras entre cada sensor y servidor para evitar la manipulación por parte de un atacante.

• Tener al menos cuatro niveles diferentes de permisos que permitan a los administradores de WIPS, delegar privilegios específicos de vista y administración a otros administradores.

• Tener informes automatizados (activados por eventos) y programados.

• Proporcionar informes personalizables.

• Segmentación de informes y administración basada en requerimientos empresariales.

• Produce captura de paquetes en real y se muestra directamente en las estaciones de trabajo de los analistas.

• Proporcionar captura de registro de eventos.

• Cumplir con todas las normas aplicables y Reglamentos.