HARDENING A EQUIPOS DE ULTIMA MILLA DE UNA EMPRESA DEL SECTOR DE LAS TELECOMUNICACIONES

PRESENTADO POR:
NESTOR JULIAN DIAZ FINO
JORGE LEONARDO CESPEDES REYES
JOSE CAMILO HENAO BARRERA

ASESOR TÉCNICO DE PROYECTO:
WILSON ROJAS REALES

UNIVERSIDAD EL BOSQUE
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD DE REDES TELEMATICAS
BOGOTÁ, COLOMBIA
22-11-2022

RESUMEN

El objetivo principal de este proyecto es diseñar las plantillas de hardening, en equipos de última milla para una empresa de telecomunicaciones; para ello, se ha realizado un análisis de la situación actual del proceso de instalación y configuración de los equipos, identificando las debilidades administrativas y de riesgos de seguridad, estas debilidades son mitigadas con controles basadas en las buenas prácticas. Para la materialización de la base de seguridad se utiliza los controles propuestos en las plantillas hardening diseñadas. En el presente trabajo se realiza un estudio de los equipos más usados en la compañía, agrupándolos en un plan de mitigación y proponiendo cada una de las plantillas por fabricante, analizando cada control sugerido por las plantillas y recomendando la adopción de los controles a la compañía.

Las líneas base de seguridad obtenidas de la comparativa de controles, comprenden la estructura principal para la aplicación del proceso de aseguramiento de los equipos que se estudian en este trabajo, esta propuesta cuenta con tres pasos que son: 1. Obtener información sobre los equipos de última milla más usados, 2. Aplicar plantillas de controles de mitigación de riesgos, 3. Emitir las recomendaciones pertinentes para el tratamiento de los posibles riesgos que puedan impactar la compañía. Los resultados de este documento muestran que la línea de base de seguridad es mejor cuando tiene diferentes puntos de vista sobre los controles estudiados, lo que proporciona la ayuda para crear un nivel más avanzado de seguridad en los equipos relacionados en el documento, para su correcto funcionamiento en la compañía.

PALABRAS CLAVE

Hardening, equipos de última milla, Seguridad, Networking, Telecomunicaciones.

ABSTRACT

The main objective of this project is to design the hardening templates, in last mile equipment for a telecommunications company; To this end, an analysis of the current situation of the equipment installation and configuration process has been carried out, identifying administrative weaknesses and security risks. These weaknesses are mitigated with controls based on good practices. For the materialization of the security base, the controls proposed in the designed hardening templates are used. In the present work a study of the most used equipment in the company is carried out, grouping them in a mitigation plan and proposing each one of the templates by manufacturer, analyzing each control suggested by the templates and recommending the adoption of the controls to the company.

The security baselines obtained from the comparison of controls comprise the main structure for the application of the assurance process of the equipment studied in this work. This proposal has three steps: 1. Obtain information about the security equipment. most used last mile, 2. Apply risk mitigation control templates, 3. Issue the pertinent recommendations for the treatment of possible risks that may impact the company. The results of this document show that the security baseline is better when you have different points of view on the studied controls, which provides the help to create a more advanced level of security on the equipment related in the document, for its correctness. operation in the company.

KEYWORDS

Hardening, computer equipment, Security, Networking, Telecommunications

Tabla de Contenido

1. Título

HARDENING A EQUIPOS DE ULTIMA MILLA DE UNA EMPRESA DEL SECTOR DE LAS TELECOMUNICACIONES.

2. Introducción

En la era digital en la que actualmente vivimos todos los seres humanos estamos compartiendo información en cada segundo de nuestras vidas y las empresas también transmiten sus datos por medio de la tecnología actual. ¿Pero que nos garantiza que esta información sólo es observada por el remitente y el emisor? Actualmente son pocas las empresas que pueden garantizar que este proceso de información sea 100% seguro, por lo cual es importante conocer qué tan vulnerables son los equipos con los que cuenta la entidad y el cliente; por donde es observada la información y cómo se pueden prevenir posibles ataques de ciberseguridad. Si una entidad no tiene claro este proceso o sus posibles lados vulnerables, son empresas más susceptibles de ataques y de pérdida total de la información lo cual puede derivarse en consecuencias económicas y legales que puede implicar esta pérdida.

Diariamente se hace uso de la informática por medio de diferentes medios tecnológicos (computador, Tablet, celular etc.) en donde se está emitiendo diversa cantidad de información personal, de entidades o grandes multinacionales; pero que tan protegido se encuentra esta información frente a diferentes ataques cibernéticos.

Toda organización que maneje datos o información sensible debe implementar un sistema de seguridad para asegurar la protección de dicha información, por lo que el Harding es una de las herramientas más productivas para brindar una solución a las organizaciones y proteger la información, ya que esta nos permite delimitar por barreras de protección tanto internas como externas dependiendo desde qué área está siendo atacada la información.

El Hardening es definido como "La implementación de la seguridad en un sistema informático" que es el planteamiento de este proyecto en la entidad de conectividad, ya que es la encargada de "brindar experiencias increíbles para el cliente con soluciones de redes, nubes y seguridad que impulsan las aplicaciones de negocios de última generación" partiendo de este planteamiento, se determinará qué tan eficaces son los equipos de la entidad, que permita garantizar el adecuado funcionamiento del Harding en la entidad y a su vez con los clientes a los que se les está prestando el servicio.

3. Descripción general del proyecto

3.1 Definición del problema

La Compañía de telecomunicaciones es proveedora de servicios de conectividad y tecnología, y presta sus servicios a clientes de distintos sectores en Colombia. Cuentan con diferentes mecanismos que permiten el abastecimiento de información, debido a esto se identifican en diferentes métodos que provocan vulnerabilidades de seguridad, para la identificación de cada uno de estos métodos el más relevante y preocupante, es que todo dispositivo electrónico tiene alguna vulnerabilidad o falla de seguridad y que algún evento o situación la pueden aprovechar

para afectar la confidencialidad, integridad y/o disponibilidad de algún servicio o información que reside en él, en los equipos de telecomunicaciones que se está ingresando y modificando dicha información pueden ser de diferentes marcas, sistemas operativos y años de vigencia, cada uno de ellos es vulnerable a un ataque tanto interno como externo como puede ser accesos inseguros o desactualizados en los equipos de redes, los sistemas operativos, configuraciones incorrectas y firmware desactualizados o algún daño físico por falta de algún mantenimiento a los equipos.

La empresa de telecomunicaciones suministra equipos de última milla a sus clientes. Estos equipos en muchas ocasiones no son configurados previamente de manera óptima. Por lo general, tal como es adquirido por parte del proveedor es instalado con una configuración con unos parámetros estándar al cliente final y dejando muchos parámetros por defecto, que no afectan su funcionalidad, pero si pueden ser generadores de riesgos de amenazas grandes.

3.2 Aspectos a solucionar

Teniendo en cuenta que los equipos de comunicaciones presentan una configuración muy básica se requiere plantear una serie de recomendaciones encaminadas al endurecimiento de los mismos equipos, esto se consigue aplicando una serie de controles basados en una plantilla de Hardening.

Colocar estos controles, permitiría mejorar los niveles de seguridad no solamente para el cliente sino también para la propia empresa que los provee. Además, se logra obtener buenas prácticas con respecto a la preparación de los equipos suministrados al cliente final. Concientizar a las diversas áreas operativas la importancia de la seguridad de la información en las redes telemáticas de manera preventiva y oportuna.

3.3 Solución propuesta

De acuerdo con el análisis realizado a la empresa de telecomunicaciones, se plantea realizar un estudio previo acerca de los diferentes equipos de última milla que la compañía adquiere y distribuye. Con base en dicho estudio, se plantea diseñar una serie de plantillas de Hardening acorde a cada tipología de equipo y por último una serie de recomendaciones con el fin de aplicar la plantilla de Hardening respectiva, para así garantizar un sistema más seguro y eficaz para la empresa y sus clientes.

4. Estado del arte

4.1 Marco de referencia teórico

De acuerdo con los avances tecnológicos que se han tenido en los últimos años; podemos identificar que muchas entidades poseen un agente que permite la detección de virus y Malware "Sistema de detección y prevención de intrusos (IDS-IPS)" el cual está acompañado por un antivirus que ayuda al bloqueo de estas amenazas. Por este motivo es necesario conocer que investigaciones o acciones han tomado a lo largo de la historia para prevenir estos agentes ya que existen desde el momento de la creación del internet.

A principio de los años 90 se generó una necesidad debido a las diferentes técnicas de ataques *"Deception Techniques Methods, honeypots, Honeynets and Usage",* que se generaban en esa época y publicaron " *The Cuckoo´s Egg: Tracking a Spy Through the maze of computer espionage"*

y *"An evening with berferd in wich a cracker is lured"* en las cuales dieron herramientas para iniciar una protección para estos ataques que algunas entidades estaban probando para dar inicio a la protección informática. (1)

En este periodo a la vez surgió el término "Honey Pot" que se define como sistema de carnada o señuelo, el cual es una herramienta de seguridad que detecta y obtiene información del atacante, por lo que podemos concluir que en los años 90 dieron el primer acercamiento a la seguridad informática por diferentes tipos de protección que permitieron seguir avanzando en ellos. (1)

En 1999 se reconoció "The Honeynet Project" en donde resaltaron la importancia y la efectividad de este sistema y complementaron la seguridad de la información. (2)

En el 2011 la tesis " Diseño e implementación de un esquema de seguridad perimetral para redes de datos caso práctico" de los autores Jose Baltazar y Juan campusanos; donde analizan unas políticas para la seguridad para adquirir en un sistema informático, basándose en buenas prácticas de administración de la seguridad con base en los estándares, seguridad en redes, Backups y protección frente a los dispositivos removibles y pentesting; A la vez respaldan el Hardening en sistemas operativos Microsoft y Unix-Linux en las que exploran las herramientas y técnicas aceptables para la seguridad informática (3)

En este mismo año la investigación "Desarrollo de una guía para selección y endurecimiento (Hardening) de sistemas operativos para un centro de datos" de Omar Sánchez; Especifica la normatividad que se puede implementar en el aseguramiento de sistemas teniendo en cuenta la NIST e ISO 15408 y como estas apoyan el desarrollo preliminar de la guía de Hardening a partir del estándar FSI generando los procedimientos operativos (POE), para ir mejorando este tipo de seguridad informática. (4)

En el 2015 Javier Robayo publicó "Aseguramiento de los sistemas computacionales de la empresa sitiosdima.net"; En donde implementaron un proceso de Hardening por medio del aseguramiento del sistema operativo Windows, se basaron en medidas de seguridad para este sistema operativo. De igual manera el Hardening por fuera de Windows como la implementación de IDS, sistema de contraseñas seguras y buenas prácticas de informática. (5)

En el 2016 publicaron "Estudio sobre la aplicación de Hardening para mejorar la seguridad informática en el centro técnico laboral de Tunjacotel" Fache J; Analiza e indaga las medidas de seguridad del Hardening en Windows y Linux describiendo sus características, ventajas y uso de las mismas y termina dando a conocer las recomendaciones y la propuesta para mejorar el tipo de seguridad informática que poseen. (6)

En el 2018 publicaron "Hardening a equipos críticos de la parte transaccional web de una entidad financiera" Carlos Morales; Identifico y analizo las amenazas que estaba expuesta la entidad y las minimizó para así exponer un Hardening a servidores críticos e implementarlo. (7)

ANTECEDENTES de la empresa de telecomunicaciones:

El enfoque actual para asegurar el acceso a los dispositivos Cisco utilizados en los servicios administrados se ha basado tradicionalmente en limitar el acceso a la aplicación de un enrutador mediante la aplicación de ACL a la aplicación o al recurso en sí (8). Ejemplos de esta práctica son:

El acceso CLI remoto está controlado por la línea ACL estándar de VTY, la aplicación utilizada para el acceso remoto está definida por el recurso VTY, SSH, por ejemplo. La ACL solo define las fuentes para la conexión entrante y no la interfaz de destino.

El acceso a SNMP a través del acceso SNMPv2 se define mediante una ACL aplicada al comando que proporciona ese recurso.

Sin embargo, la exposición a otras aplicaciones, como protocolos de enrutamiento, ICMP, etc., no se controla explícitamente a través de ACL específicas de la aplicación y, fundamentalmente, permanece abierta. Cisco IOS no emplea un envoltorio TCP/UDP completo para los servicios, por lo que es posible consumir recursos en el dispositivo que no debería estar disponible

Para mitigar la exposición a recursos sin ACL explícitas, se debe aplicar una capa adicional de configuración para mitigar el riesgo de acceso no solicitado. Cisco IOS no emplea el concepto de un firewall interno, sino que requiere el uso de ACL basadas en interfaz (ACL de infraestructura) y controles de recursos adicionales mediante el uso de un controlador de plano de control.

Cisco documentó los defensores de las mejores prácticas de refuerzo de enrutadores para la creación e implementación de ACL extendidas de entrada específicas que solo permiten explícitamente el tráfico destinado al dispositivo en direcciones de destino específicas por interfaz y prohíben todo el otro tráfico no deseado destinado al dispositivo.

Las ACL de infraestructura se crean a partir del uso de ACL extendidas de IOS y no tienen ningún concepto del estado de inicio de TCP más allá de identificar algo como establecido. Las ACL de Cisco IOS no se pueden anidar ni hacer referencia a ACL adicionales y, por lo tanto, se debe mantener una ACL de infraestructura de forma independiente.

La aplicación de una IACL es una base específica de la interfaz, pero también debe tener en cuenta la comunicación adicional a las interfaces internas, como las interfaces de bucle invertido para la gestión, según sea necesario. Las ACL de interfaz aplicadas a los dispositivos administrados también deben atender la gran cantidad de cambios en la infraestructura de administración dentro de la misma construcción de ACL.

4.2 Marco de referencia tecnológico

En el mercado o en el nicho de las telecomunicaciones, existen diversos fabricantes que proveen equipos de conectividad, con sus series y modelos respectivos, dichos equipos son unos de los más utilizados por los proveedores de telecomunicaciones, entre los que se pueden mencionar los siguientes:

- ROUTER CISCO 1000 SERIES (9)

Cisco es la plataforma que ofrece los enrutadores de servicios integrados (ISR) de la serie 1000, y es la más adecuada para pequeñas y medianas empresas, sucursales empresariales y como equipo en las instalaciones del cliente en entornos de servicios administrados. Ofrece un alto rendimiento con múltiples servicios mediante una arquitectura multinúcleo, ahorra en costos operativos con Cisco SD-WAN y licencias de pago a medida que crece.

Ofrece las últimas tecnologías inalámbricas, como 5G para conectividad de WAN inalámbrica y 802.11ac o 802.11ax (Wi-Fi 6) para LAN inalámbrica con funcionalidad *Mobility Express* completa.

Aumenta la seguridad con soluciones confiables de Cisco, arranque seguro, anclaje de hardware, identificador único de dispositivo seguro (SUDI), defensas en tiempo de ejecución, verificación de integridad y análisis de tráfico cifrado.
Bloquea los ataques maliciosos de phishing y malware en la sucursal con la seguridad de Cisco Umbrella.

- ROUTER CISCO 4000 SERIES (10)

Los routers de servicios integrados (ISR) Cisco Serie 4000 están diseñados para organizaciones que poseen numerosas sucursales y oficinas remotas. Las sucursales actuales ofrecen servicios completos a través de aplicaciones en la nube, móviles y multimedia, y exigen mayor comunicación directa tanto con Data Centers privados como con nubes públicas a través de VPN e Internet. También necesitan un reducido coste total de propiedad (TCO) para su hardware de red.
Características: Clave de la nueva arquitectura Los routers ISR de Cisco serie 4000 incluyen varias características importantes que los convierten en la elección perfecta para las sucursales modernas:
Precio por rendimiento: el Cisco serie 4000 permite a las sucursales adaptarse al aumento del ancho de banda usando un solo dispositivo sin necesidad de dispositivos de seguridad y optimización, lo que ayuda a controlar los costes.
Rendimiento según demanda (pague según uso): las sucursales remotas pueden actualizarse a un nivel de ancho de banda superior sin tener que adquirir un dispositivo nuevo.
Servicios ampliables: los routers Cisco serie 4000 son compatibles con los servidores Cisco Unified Computing System™ (Cisco UCS®) serie E Blade, comparables a un servidor de tamaño completo.

- ROUTER JUNIPER SERIES SRX100 (10)

El SRX110 Services Gateway ofrece una plataforma de red y seguridad única, consolidada y rentable para sucursales pequeñas. Cuenta con una interfaz WAN VDSL/ADSL2+ integrada, capacidades 3G/4G y un conmutador Fast Ethernet de 8 puertos.

La serie SRX para la sucursal son Services Gateway de seguridad de próxima generación que brindan capacidades esenciales que conectan, protegen y administran ubicaciones de la fuerza laboral con un tamaño que va desde unos pocos hasta cientos de usuarios. Al consolidar capacidades de firewall, enrutamiento, seguridad y conmutación rápida y de alta disponibilidad en un solo dispositivo, las empresas pueden proteger sus recursos y brindar económicamente nuevos servicios, conectividad segura y una experiencia satisfactoria para el usuario final. Todas las puertas de enlace de servicios de la serie SRX, incluidos los productos escalados para las aplicaciones Enterprise Branch, Enterprise Edge y Data Center, cuentan con la tecnología de Junos OS, el sistema operativo comprobado que proporciona una consistencia inigualable, un mejor rendimiento con los servicios y una protección superior de la infraestructura a un costo total más bajo. de propiedad.

La serie SRX de Juniper Networks para la sucursal combinan el firewall de próxima generación y los servicios de administración unificada de amenazas (UTM) con enrutamiento y conmutación en un único dispositivo de red rentable y de alto rendimiento.

La serie SRX para la sucursal ejecuta el sistema operativo Juniper Networks Junos, el sistema operativo probado que utilizan los principales enrutadores de Internet en los 100 principales proveedores de servicios del mundo. Las funciones de enrutamiento de clase portadora rigurosamente probadas de IPv4/IPv6, OSPF, BGP y multidifusión se han probado en más de 15 años de implementaciones en todo el mundo.

La serie SRX para la sucursal proporciona seguridad perimetral, seguridad de contenido, visibilidad de aplicaciones, seguimiento y cumplimiento de políticas, control basado en roles de usuario, inteligencia de amenazas a través de la integración con Juniper Networks Spotlight Secure* y visibilidad y control de amenazas en toda la red. Usando zonas y políticas, los administradores de red pueden configurar e implementar puertas de enlace de la serie SRX de sucursal de forma rápida y segura. Las VPN basadas en políticas admiten arquitecturas de seguridad más complejas que requieren direccionamiento dinámico y tunelización dividida. La serie SRX también incluye asistentes para firewall, IPsec VPN, traducción de direcciones de red (NAT) y configuración inicial para simplificar las configuraciones desde el primer momento.

Para la seguridad del contenido, la serie SRX para la sucursal ofrece un conjunto completo de firewall de próxima generación, administración unificada de amenazas (UTM) y servicios de inteligencia de amenazas que consisten en: sistema de prevención de intrusiones (IPS), seguridad de aplicaciones (AppSecure), controles de firewall basados en roles de usuario , antivirus integrado y basado en la nube, antispam y filtrado web mejorado para proteger su red de las últimas amenazas transmitidas por contenido. La inteligencia de amenazas integrada a través de Spotlight Secure ofrece protección contra amenazas adaptable contra botnets relacionados con comando y control (C&C) y aplicación de políticas basadas en GeoIP y tecnología de huellas dactilares de atacantes (esta última para protección de aplicaciones web), todo lo cual se basa en fuentes proporcionadas por Juniper. Los clientes también pueden aprovechar sus propios feeds personalizados y de terceros para protegerse contra malware avanzado y otras amenazas. La serie SRX para sucursales se integra con otros productos de seguridad de Juniper para ofrecer control de acceso unificado (UAC) en toda la empresa y gestión adaptable de amenazas.

- ROUTER SDWAN CISCO MERAKI SERIES MX (12)

Meraki ofrece soluciones de TI completas, escalables e intuitivas para la gestión en la nube como Puntos de Acceso (MR), Switches (MS), Dispositivos de Seguridad (MX), Software de administración de dispositivos (SM), Cámaras de Seguridad (MV) y Meraki Insight (MI). Hardware, software y servicios en la nube integrados, todo administrado a través de un panel de control basado en el web llamado Dashboard.

Los dispositivos de seguridad y SD-WAN Cisco Meraki MX son ideales para organizaciones que planean una solución de administración unificada de amenazas (UTM) para sitios distribuidos, campus o concentración de VPN de centro de datos. Como MX se administra 100% en la nube, la instalación y la administración remota son muy simples. MX cuenta con un paquete integral de

servicios de red, lo cual elimina la necesidad de usar varios dispositivos. Estos servicios incluyen funcionalidades de SD-WAN, firewall basado en aplicaciones, filtrado de contenido, filtrado de búsqueda web, detección y prevención de intrusiones basadas en SNORT®, protección avanzada contra malware (AMP), almacenamiento en caché web y conmutación por falla de red celular 4 G, entre muchos otros. Las características de SD-WAN y VPN automática están disponibles en nuestros dispositivos virtuales y componentes de hardware, y se pueden configurar en Amazon Web Services o Microsoft Azure.

Control de tráfico con reconocimiento de aplicaciones: las políticas de ancho de banda para tipos de aplicaciones de capa 7 (p. ej., bloquear YouTube, priorizar Skype, limitar BitTorrent). • Filtrado de contenido: filtro de contenido conforme a CIPA, aplicación de búsqueda segura (Google/Bing) y YouTube para escuelas.

- Prevención de intrusiones: sensor IPS conforme a PCI, con base de datos de firmas SNORT®, líder del sector, de Cisco.

Protección avanzada contra malware:

- motor de protección basado en la reputación de archivos con tecnología de Cisco AMP.
- Políticas de seguridad y administración de aplicaciones según identidades.

5. Glosario de términos

Vulnerabilidades: Toda aquella debilidad que presente un software o hardware, que puede ser explotada por un ataque cibernético para acceder de forma no autorizada al sistema informático. tiene un diseño gráfico muy amigable para el usuario

Amenazas: Las amenazas informáticas son aquellas ocasiones en que piratas informáticos lograron entrar en tus computadoras, dispositivos y/o servidores con malas intenciones. Estos ataques, dependiendo de cuál sea, pueden darse a través de e-mails engañosos, haciendo clic en anuncios maliciosos, etc.

Ciberseguridad: Conjunto de elementos, medidas y equipos destinados a controlar la seguridad informática de una entidad o espacio virtual.

Redes telemáticas: Conjunto de elementos que permiten que varios dispositivos intercambien datos entre sí. Este intercambio se realizará a través de un medio 'físico'.

Telecomunicaciones: Es toda transmisión, emisión o recepción, de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos".

Riesgos informáticos: En arquitectura de computadores, un riesgo es un problema potencial que puede ocurrir en un procesador segmentado. Típicamente los riesgos se clasifican en tres tipos: riesgos de datos, riesgos de salto o de control y riesgos estructurales.

Análisis de riesgos: es el uso sistemático de la información disponible para determinar la frecuencia con la que determinados eventos se pueden producir y la magnitud de sus consecuencias.

Confidencialidad: es la garantía de que la información personal será protegida para que no sea divulgada sin consentimiento de la persona. Dicha garantía se lleva a cabo por medio de un grupo de reglas que limitan el acceso a esta información, acceso a la información solo mediante autorización y de forma controlada.

Disponibilidad: En términos de seguridad de la información, la disponibilidad hace referencia a que la información del sistema debe permanecer accesible a elementos autorizados

Integridad: En términos de seguridad de la información, la integridad hace referencia a la fidelidad de la información o recursos, y normalmente se expresa en lo referente a prevenir el cambio impropio o desautorizado.

Política de seguridad: Es un conjunto de reglas que se aplican a las actividades del sistema y a los recursos de comunicaciones que pertenecen a una organización. Estas reglas incluyen áreas
como la seguridad física, personal, administrativa y de la red.

Hardening: En informática, el hardening o endurecimiento es el proceso de asegurar un sistema reduciendo sus vulnerabilidades o agujeros de seguridad, para los que se está más propenso cuantas más funciones desempeña; en principio un sistema con una única función es más seguro que uno con mucho propósito.

Redes: Es un grupo sistemático de canales o de hilos conductores o de vías de comunicación o de agencias y servicios o recursos para determinado fin.

Router: Un router, enrutador o encaminador es un dispositivo que permite interconectar redes con distinto prefijo en su dirección IP. Su función es la de establecer la mejor ruta que destinará a cada paquete de datos para llegar a la red y al dispositivo de destino.

SDWAN: Una red de área extensa definida por software (SD-WAN) es una arquitectura de WAN virtual que permite a las empresas aprovechar cualquier combinación de servicios de transporte, incluidos MPLS, LTE y servicios de Internet de banda ancha, para conectar de forma segura a los usuarios con las aplicaciones

Access Control Lists (ACL): Las Listas de Control de Accesos proveen de un nivel de seguridad adicional a los clásicos provistos por los Sistemas Operativos. Estas listas permiten definir permisos a usuarios y grupos concretos. Por ejemplo, pueden definirse sobre un Proxy una lista de todos los usuarios (o grupos de ellos) a quien se le permite el acceso a Internet, FTP, etc. También podrán definirse otras características como limitaciones de anchos de banda y horarios

6. Justificación

Las organizaciones son objeto de innumerables intentos de vulneración abusiva de sus sistemas, para extraer su información por parte de delincuencia informática, muchas empresas hoy en día son víctimas de estos ataques dirigidos a su infraestructura, ya que para algunos nunca fue una de sus prioridades capacitar el personal, tomar medidas de seguridad para prevenir o minimizar los ataques.

El desarrollo de este proyecto está enfocado al aseguramiento de los sistemas de cualquier organización, es una necesidad latente preparar a las empresas ante cualquier amenaza que pueda afectar su operación, poniendo en conocimiento las diferentes herramientas disponibles en beneficio de elevar su nivel de seguridad en las plataformas y hacer una detección oportuna de las vulnerabilidades encontradas en los sistemas de telecomunicaciones.

Existen mecanismos en los que se puede visualizar paquetes, sea capaz de capturar todo el tráfico de datos, incluyendo la información de autenticación porque se realiza sin ningún tipo de cifrado. Por supuesto, cualquier archivo o comando que nosotros transfiramos o ejecutemos, se podrá ver sin ningún problema. Sin embargo, dichos riesgos, se vale de cualquier usuario que se encuentre dentro de una determinada red por ello se debe implementar las plantillas de hardening con el fin de mitigar el riesgo en las cuales son específicas para los equipos Cisco, Meraki, Juniper.

Fabricante	Porcentaje de riesgo
Cisco	80%
Juniper	12%
Cisco Meraki	5%

Con el conocimiento de las herramientas utilizadas para realizar las plantillas de hardening, se puede definir el diseño de implementación para la mitigación de las fallas de seguridad encontradas dentro de los equipos de última milla que provee la compañía de telecomunicaciones y de esta manera generar procesos que permitan hacer análisis, detección y tratamiento de vulnerabilidades de seguridad periódicamente, para prevenir ataques e intrusiones en los puntos más débiles de nuestra infraestructura.

7. Objetivos

7.1. General.

Definir recomendaciones de buenas prácticas de seguridad a partir de las plantillas de Hardening para el aseguramiento de la infraestructura tecnológica de la organización y sus clientes finales.

7.2. Específicos

- Realizar estudio previo para consolidar la información de los equipos que la compañía distribuye a sus clientes finales.
- Diseñar plantillas Hardening a partir de la información recolectada en base en las buenas prácticas de configuración.
- Realizar recomendaciones con el fin de salvaguardar la integridad, confidencialidad y disponibilidad de los equipos de última milla instalados en cliente final.

8. Requerimientos

El tipo de Investigación que contempla este proyecto es la Investigación aplicada, ya que su principal objetivo, se basa en resolver un problema práctico de gestión de vulnerabilidades en dispositivos enrutadores de última milla, con un alcance determinado y limitado. De este modo se generan pocos aportes al conocimiento científico desde un punto de vista teórico, pero se logran poner en práctica los conocimientos adquiridos en el desarrollo de cada una de estas etapas.

Recolección de Información para identificar objetivos específicos en los equipos objetivo. De acuerdo con el escenario escogido de las pruebas, se pueden dar a conocer las siguientes situaciones, en donde no se proporciona ningún tipo de información y se lleva a cabo la tarea de descubrimiento de la misma. En este escenario las pruebas toman más tiempo por cuanto se debe recolectar más información inicialmente se realizan las siguientes pruebas:

- Pruebas con Información, donde el cliente proporciona información básica de sus redes, y se puede optimizar el tiempo de pruebas orientándolas a los objetivos específicos definidos.
- Pruebas con cuenta creada y validada a nivel de un usuario nivel medio.
- Pruebas sin protección de los dispositivos (Tomando todas las precauciones para proteger los sitios a explorar).

Análisis de Vulnerabilidades. Consiste en determinar problemas de seguridad en los puntos hallados en la fase 1 Recolección de Información. Estos problemas de seguridad se pueden determinar partiendo de la investigación de los equipos encontrados con sus especificaciones y orientándolo al cuidado del mismo dispositivo o usando herramientas especializadas orientadas al análisis de vulnerabilidades específico de protocolos. Dependiendo del tipo de herramienta utilizada y la arquitectura, el análisis de las vulnerabilidades detectadas puede tardar más tiempo, ya que, para tener mayores probabilidades de éxito, es necesario determinar los falsos positivos. Como resultado del análisis de vulnerabilidades, plantean las plantillas adecuadas para cada equipo de acuerdo con la información recolectada de las vulnerabilidades posibles en los equipos.

Análisis Final. Generación de un informe detallado con los resultados obtenidos durante todo el proceso de ejecución, con el correspondiente análisis de dicha información para poder ser interpretada de manera correcta y entender las implicaciones a nivel de seguridad sobre la infraestructura tecnológica con las recomendaciones necesarias para mitigar dichos problemas de aseguramiento.

9. Metodología

El tipo de Investigación que contempla este proyecto es la Investigación aplicada, ya que su principal objetivo, se basa en resolver un problema práctico de gestión de vulnerabilidades en dispositivos enrutadores de última milla, con un alcance determinado y limitado. De este modo se generan pocos aportes al conocimiento científico desde un punto de vista teórico, pero se logran poner en práctica los conocimientos adquiridos en el desarrollo de cada una de estas etapas.

Recolección de Información para identificar objetivos específicos en los equipos objetivo. De acuerdo con el escenario escogido de las pruebas, se pueden dar las siguientes situaciones o

Pruebas Ciegas, en donde no se proporciona ningún tipo de información y se lleva a cabo la tarea de descubrimiento de la misma. En este escenario las pruebas toman más tiempo por cuanto se debe recolectar más información inicialmente se realizan las siguientes pruebas:

- Pruebas con Información, donde el cliente proporciona información básica de sus redes, y se puede optimizar el tiempo de pruebas orientándolas a los objetivos específicos definidos.
- Pruebas con cuenta creada y validada a nivel de un usuario nivel medio.
- Pruebas sin protección de los dispositivos de protección de perímetro (Tomando todas las precauciones para proteger los sitios a explorar).

Análisis de Vulnerabilidades. Consiste en determinar problemas de seguridad en los puntos hallados en la fase 1 Recolección de Información. Estos problemas de seguridad se pueden determinar usando herramientas especializadas orientadas al análisis de vulnerabilidades específico de protocolos. Dependiendo del tipo de herramienta utilizada y la arquitectura, el análisis de las vulnerabilidades detectadas puede tardar más tiempo, ya que, para tener mayores probabilidades de éxito, es necesario determinar los falsos positivos. Como resultado del análisis de vulnerabilidades, plantean las plantillas adecuadas para cada equipo de acuerdo con la información recolectada de las vulnerabilidades posibles en los equipos.

Análisis Final. Generación de un informe detallado con los resultados obtenidos durante todo el proceso de ejecución, con el correspondiente análisis de dicha información para poder ser interpretada de manera correcta y entender las implicaciones a nivel de seguridad sobre la infraestructura tecnológica con las recomendaciones necesarias para solucionar dichos problemas de aseguramiento.

10. Capítulos de desarrollo

Se realiza el levantamiento de información acerca de los equipos de última milla de la empresa de telecomunicaciones que actualmente están en producción en los clientes finales, el cual nos proporciona una visibilidad de las marcas de fabricantes que más se están utilizando para su implementación, logrando enfocar las plantillas de Hardening para los dispositivos que tienen características de enrutadores de tráfico de datos e internet y que van de la mano con una configuración acorde a las necesidades que el cliente contrata.

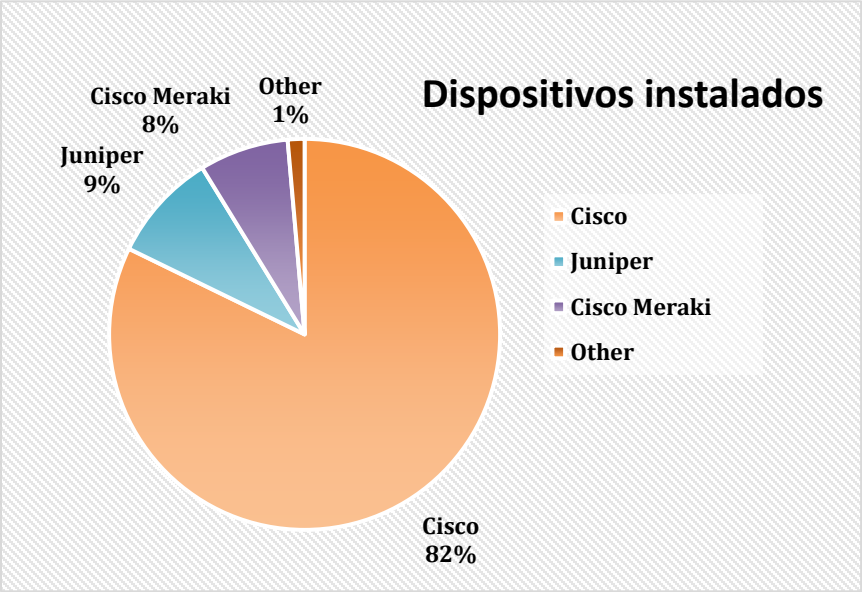
Listado de equipos en la compaña

En un listado interno de clientes de la compañía telecomunicaciones (14) con corte a septiembre de 2022, tomamos una muestra de la región y realizamos el filtrado de los equipos de última milla que están en producción para los servicios que ofrecen conectividad. Se puede observar que son mayoritariamente de los fabricantes Cisco, Juniper y Cisco Meraki, los cuales proporcionan tanto el hardware como el software para los servicios que ofrece la compañía.

Fabricante	Número de dispositivos	Porcentaje
Cisco	1780	82%
Juniper	195	9%
Cisco Meraki	160	7%

Otros	30	1%
Total	2165	100%

(14)



(15)

De la anterior tabla (15), se observa que el fabricante Cisco tiene la mayor proporción de dispositivos instalados de las tres marcas más relevantes con un 82%, seguido de Juniper con un 9%, y SDWAN con Cisco Meraki con una participación del 7.4%. Éste último está teniendo una proyección de crecimiento muy alto en los próximos años, ya que es la nueva generación de equipos de última milla.

Listado de equipos por series.

Fabricante	Número de Equipos	Porcentaje
Cisco		82%
Series 1000	948	
Series 4000	832	
Cisco SDWAN Meraki		7%
Series MX	160	
Juniper		9%
Series SRX 100	195	
Otros		1%
N/A	30	
Total	2165	100%

(16)

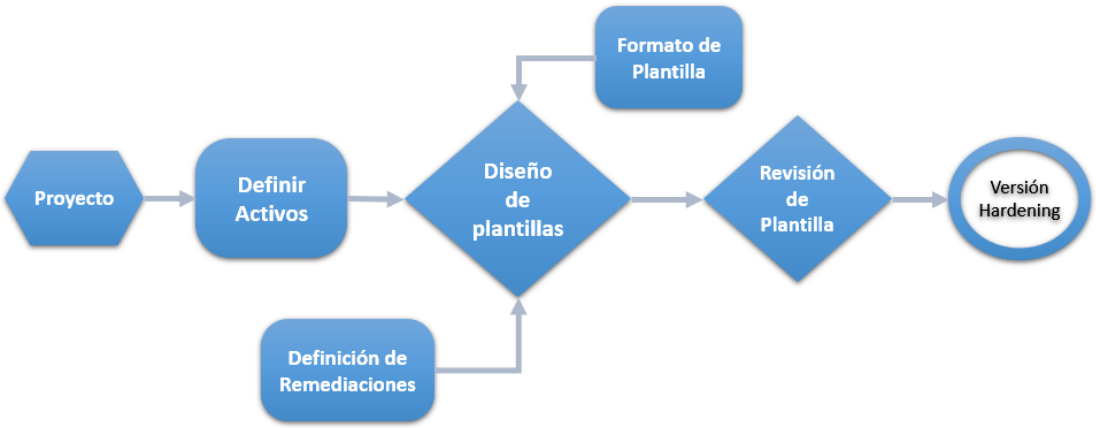
Del fabricante Cisco se tienen dos series importantes de dispositivos en producción, los cuales son las series 1000 y series 4000. Del fabricante Juniper, la serie SRX 100 y de Cisco Meraki la series

MX (16).

De acuerdo con el levantamiento de información realizado acerca de los equipos de última milla que más se emplean en las implementaciones, podemos determinar que los diseños de las plantillas de Hardening son tres, los cuales están conformados por el fabricante Cisco, Juniper y Cisco Meraki. Cada uno de estos hardening abarcará las líneas o series de equipos que actualmente se implementan en la compañía. Del fabricante Cisco la plantilla de hardening puede ser aplicada a los equipos de última milla, Series Cisco ISR 1000 y 4000, ya que está basada en las buenas prácticas de última versión de IOS 17.x, documentadas en *CIS Cisco IOS 17.x Benchmark v1.0.0*; para los equipos Juniper la plantilla de hardening está basada en las buenas prácticas de la versión genérica de Juniper OS (documentadas en *CIS Juniper OS Benchmark v2.1.0*), y para los equipos SD-WAN Cisco Meraki están basados en la versión de firmware estable MX 16.16.x. Las plantillas hardening a diseñar contemplan los temas de riesgos y recomendaciones de mitigación generales que tienen en común estos equipos, y puedan ser implementadas en la configuración de manera precisa.

Contemplamos el siguiente flujo de trabajo para el diseño de las plantillas de Harding (17).

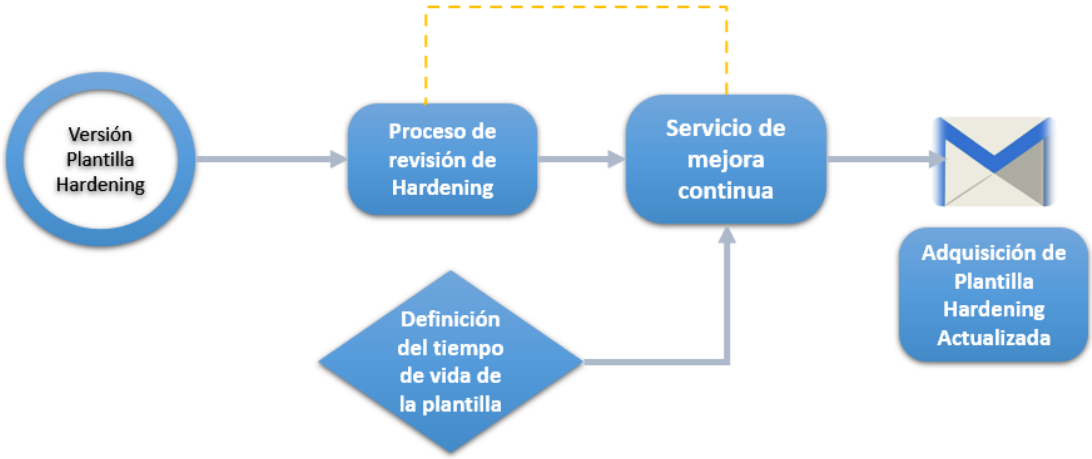
Flujo de trabajo para el diseño de la plantilla de Hardening



(17)

Cabe destacar que cada plantilla es susceptible de actualizaciones periódicas, ya que estas tienen un ciclo de vida debido a actualizaciones del firmware de los equipos que obligan, en el caso de los equipos Cisco y Juniper, a nuevas versiones en los documentos de CIS Benchmarkm y en cisco Meraki en su web *General MX Best Practices Meraki*.

Flujo de ciclo de vida de la plantilla



El diseño de la plantilla de Hardening se toma como referencia de un formato simplificado (Anexo 2) de fácil lectura y comprensión, brindándole al personal técnico con conocimiento en estos sistemas, una mejor aplicación cuando realice la configuración de las remediaciones que se recomiendan la plantilla, disminuyendo posibles errores humanos al tener las plantillas una descripción paso a paso en cada parámetro de la configuración.

En su encabezado la plantilla de hardening (19) tiene los campos necesarios para tener un detalle de la identificación del equipo de última milla al cual se va a aplicar la plantilla, siendo los siguientes:

- Título: diligenciar el fabricante del equipo, su modelo y el identificador único que tenga *CHECKLIST– HARDENING –* (*FABRICANTE_MODELO_EQUIPO_IDENTIFICADOR*)
- Equipo: diligenciar el nombre del equipo (*Modelo_Identifiacador*).
- Dirección IP: diligenciar la dirección IP del equipo.
- Función: Que rol desempeña el equipo dentro de la organización a la que pertenece
- Responsable del equipo: área o grupo responsable del equipo.
- Versión de IOS/Firmware: se debe diligenciar la versión del IOS o Firmware el cual tiene el equipo.
- Fecha/Hora: diligenciar la fecha y hora en la cual se aplica la plantilla de hardening
- Duración: diligenciar la duración de la actividad de aplicación del hardening.

CHECKLIST– HARDENING – (FABRICANTE_MODELO_EQUIPO_IDENTIFICADOR)

EQUIPO:		FECHA: HORA: DURACIÓN:
DIRECCIÓN IP:		
FUNCIÓN DEL EQUIPO:		
RESPONSABLE DEL EQUIPO:		
VERSION DE IOS/ FIRMWARE:		

(Anexo 19)

En su cuerpo la plantilla de hardening tiene una estructura que agrupa los temas, dos casillas de chequeo si es exitosa o no, la configuración de remediación, parámetros o componente que está siendo afectado, valor o cambio para implantar, en el cual resume la recomendación, y finalmente el procedimiento para su implantación que detalla paso a paso de la configuración.

Tema:	1.			
Ejecutada/ Exitosa		***Parámetro / Componente***	***Valor o cambio para implantar***	***Procedimiento para su implantación***
SI	NO			

Al final de la plantilla de hardening se dispone de un campo para documentar las observaciones que se tengan cuando se culmine la aplicación de la plantilla al equipo implicado.

CHECKLIST– HARDENING – (FABRICANTE_MODELO_EQUIPO_IDENTIFICADOR)

Tema	***Observaciones***

Amenazas y Brechas de seguridad

Se analiza una lista de amenazas posibles que pueden afectar estos equipos de última milla y pueden estar latentes por diversos factores. Uno de los factores más importantes está en las configuraciones que tienen estos equipos de manera inicial al momento de implementarse y entregar al cliente. Dichas configuraciones presentan algunos apartados de configuración por defecto, sin atender, los cuales son brechas de seguridad que potencian estas amenazas si no son debidamente identificadas. Para esto debemos tener buenas prácticas en las configuraciones que incluso en la mayoría de los casos los fabricantes de estos equipos las proveen.

Las compañías tanto proveedoras de servicios de telecomunicaciones como las que contratan estos servicios, sus activos más importantes dependen en gran parte de estos equipos de comunicaciones. La intrusión de personal no autorizado a la red puede hacer surgir uno o varios de los tipos amenazas como puede ser el robo de información, manipulación de datos, interrupción del servicio, robo de identidad o credenciales que cualquiera de estos tendría efectos devastadores.

- Amenazas internas: esta es la más común, siendo un 70 % de las amenazas más recurrentes que provienen del interior de la organización, son muy conocidas como insiders y tiene como actores principales a los empleados actuales o exempleados, socios comerciales contratistas y/o proveedores.

- Robo de información: es una de las amenazas que tiene impacto directo sobre uno de los activos más importantes de la compañía, y se considera una de las más graves ya que al ser vulnerados los quipos de comunicación, pueden llegar a interceptar para beneficios mal intencionados ocasionando pérdidas económicas.

- Amenazas físicas: La seguridad física es la protección de los sistemas y equipos frente a amenazas de tipo tangibles. Para ello, se crean barreras y mecanismos de control y prevención como respuesta a las posibles amenazas de seguridad física, tales como, Desastres naturales, Sabotajes ajenos o internos y Fallos en las condiciones de seguridad ambienta

- Manipulación de datos: Un atacante o intruso puede manipular o modificar la información de la compañía si no si no se tienen los equipos de última milla correctamente asegurados causando impactos negativos.

- Interrupción del servicio: La interrupción de servicios en los sistemas de comunicaciones puede impedir que usuarios legítimos puedan acceder a estos que tienen derecho, comúnmente la denegación de servicios en los dispositivos de comunicaciones como servidores, o enlaces de red, provocan pérdidas económicas importantes.

- Robo de identidad: EL robo de identidad es la manera que se roban información personal con el fin de apoderarse de la identidad de alguien, al pasarse por otro individuo legitimo puede acceder a datos acceso sensibles de la compañía de telecomunicaciones.

Este grupo de amenazas engloba las más comunes y muy ligadas con las brechas de seguridad presentes en los equipos de última milla en sus configuraciones iniciales, sin un tratamiento a enfocado a la seguridad, dejando configuraciones por defecto sin revisión. Por eso, al realizar un análisis de la configuración inicial de los equipos en el momento de su instalación y entrega al cliente, pudimos recolectar las siguientes brechas de seguridad que más se repiten y tienen una relevancia muy importante.

Tabla de brechas de seguridad por fabricante

Brechas de seguridad	Afectación		Fabricantes afectadas		
			Cisco	Juniper	Cisco Meraki
Acceso físico a los equipos por personal no autorizado	Integridad	X	X	X	X
	Confidencialidad	X			
	Disponibilidad	X			
Condiciones de instalación físicas con riesgo eléctrico y ambiental.	Integridad		X	X	X
	Confidencialidad				
	Disponibilidad	X			
Imágenes de software o firmware desactualizados.	Integridad	X	X	X	X
	Confidencialidad	X			
	Disponibilidad	X			

Equipo en producción, sin soporte por el fabricante o fuera de su vida útil.	Integridad	X		X	
	Confidencialidad	X			
	Disponibilidad	X			
Licencias de equipos de vencidas.	Integridad		X	X	X
	Confidencialidad				
	Disponibilidad	X			
Copias de configuración desactualizadas en las plataformas empleadas para este fin.	Integridad		X	X	x
	Confidencialidad				
	Disponibilidad	X			
Sistema de alarmas automáticas de eventos no configurado.	Integridad				X
	Confidencialidad				
	Disponibilidad	X			
Se encontró activo el protocolo Telnet, a pesar de tener control del acceso CLI mediante una línea ACL estándar en la línea VTY y tener activo el protocolo SSH.	Integridad		X	X	
	Confidencialidad	X			
	Disponibilidad				
Se han encontrado varias interfaces Loopback configuradas en lo enrutadores	Integridad		X	X	
	Confidencialidad	X			
	Disponibilidad				
En muchos equipos no está habilitado el protocolo SSH.	Integridad		X	X	
	Confidencialidad	X			
	Disponibilidad	X			
Se evidencia que en algunos dispositivos las claves no son mayores a 2048 bits.	Integridad		X	X	
	Confidencialidad	X			
	Disponibilidad	X			
Contraseñas de acceso local con baja complejidad.	Integridad		X	X	X
	Confidencialidad	X			
	Disponibilidad				
Se ha evidenciado que algunos enrutadores no tienen configurado el protocolo NTP, encontrando por consiguiente que los registros en los enrutadores estén desincronizados; y si tienen configurado NTP, no están utilizando una ACL o una autenticación que limite las actualizaciones de hora de servidores autorizados.	Integridad		X	X	
	Confidencialidad	X			
	Disponibilidad				
Configuración de la zona de horario local del dispositivo no acorde a la región.	Integridad	X			X
	Confidencialidad				
	Disponibilidad	X			
A nivel de enrutamiento, se encontró que los vecinos BGP no están autenticados, lo que ocasiona el riesgo de que un atacante se haga pasar por un vecino BGP e inyectar información incorrecta en la tabla de rutas.	Integridad	X	X	X	
	Confidencialidad	X			
	Disponibilidad	X			
Observamos que, aunque existe una configuración de comunidades SNMPv1/v2 en modo lectura, existen comunidades predeterminadas que son comunes y bien conocidas como la comunidad "public".	Integridad		X	X	X
	Confidencialidad	X			
	Disponibilidad				
	Integridad		X	X	X

Pudimos evidenciar que en los dispositivos no está habilitado la versión de SNMPv3, la cual utiliza autenticación.	Confidencialidad	X			
	Disponibilidad				
Se observó que las comunidades SNMP no tienen habilitada una ACL para restringir el acceso a servidores de administración de confianza.	Integridad	X			
	Confidencialidad	X	X	X	
	Disponibilidad				
Redirecciones ICMP habilitados en los equipos.	Integridad	X			
	Confidencialidad	X		X	
	Disponibilidad				
Evidenciamos que algunos enrutadores a pesar de tener habilitado el control de acceso AAA, no tienen habilitado los servidores radius/tacacs que habilitan los usuarios de red en el dispositivo, lo que ocasiona que se acceda al mismo con los usuarios locales.	Integridad				
	Confidencialidad	X	X		
	Disponibilidad	X			
Se observa usuarios locales con privilegios elevados sin control.	Integridad	X			
	Confidencialidad		X	X	
	Disponibilidad	X			
No se tiene se tiene habilitado el cifrado para las contraseñas habilitadas.	Integridad				
	Confidencialidad	X	X		
	Disponibilidad				
Se evidencia que el protocolo Netflow habilitado por defecto.	Integridad				
	Confidencialidad	X			X
	Disponibilidad				
Encontramos que los enrutadores no tienen habilitado el protocolo AAA, por lo que su acceso es a través de usuarios locales.	Integridad				
	Confidencialidad	X	X	X	
	Disponibilidad	X			
Observamos que muchos dispositivos no tienen habilitado el comando "service password-encryption" para cifrar las credenciales en su configuración.	Integridad				
	Confidencialidad	X	X		
	Disponibilidad				
No utilizan nomenclatura estandarizada para la identificación del dispositivo de última milla.	Integridad				
	Confidencialidad		X	X	X
	Disponibilidad	X			
Políticas de autenticación débiles	Integridad	X			
	Confidencialidad	X	X	X	X
	Disponibilidad	X			
Se evidencia protocolo CDP habilitados en algunos dispositivos	Integridad				
	Confidencialidad	X	X		
	Disponibilidad				
Algunos enrutadores no envían sus registros Syslog a un servidor externo.	Integridad				
	Confidencialidad		X	X	
	Disponibilidad	X			
Actualización automática de firmware con versiones Beta no estables.	Integridad	X			
	Confidencialidad	X			X
	Disponibilidad	X			

Negociación de puertos de las interfaces WAN y LAN no configurado correctamente	Integridad	X			
	Confidencialidad			X	X
	Disponibilidad	X			
Se evidencia interfaces lógicamente activas en los dispositivos sin estarlas utilizando.	Integridad				
	Confidencialidad	X	X	X	X
	Disponibilidad	X			
Se evidencia proxy arp habilitado por defecto en las interfaces de los dispositivos	Integridad				
	Confidencialidad	X	X	X	
	Disponibilidad				
Roles de acceso no definidos para los usuarios de administración.	Integridad	X			
	Confidencialidad	X	X	X	X
	Disponibilidad				

Con base en la información recolectada anteriormente, y teniendo en cuenta las buenas prácticas mencionadas en el documento *CIS Cisco IOS 17.x Benchmark v1.0.0* para los modelos Cisco (20), *CIS Juniper OS Benchmark v2.1.0* para los modelos Juniper (20), y *General MX Best Practices Meraki*, se diseñan las plantillas de hardening, con los parámetros que se aconsejan cambiar y un procedimiento detallado paso a paso en la configuración del equipo, que brinda la remediación a las brechas de seguridad ya identificadas previamente.

Ejemplo:

Plantilla de Hardening

Tema:	Reglas SNMP			
Ejecutada/ Exitosa		*Parámetro / Componente*	*Valor o cambio a implantar*	*Procedimiento para su implantación*

		Deshabilitar SNMP cuando no se utilice	Si no está en uso, se debe deshabilitar el protocolo simple de administración de red (SNMP), el acceso de lectura y escritura.	Deshabilitar el acceso de lectura y escritura de SNMP si no se usa para monitorear y/o administrar el dispositivo.
				`Router(config)#no snmp-server`
				Verificar que el resultado sea "SNMP agent not enabled"
				`Router#show snmp community`
				Estado Actual SNMP: _____

		Deshabilitar 'private' en comunidad SNMP	Para reducir el riesgo de acceso no autorizado se debe deshabilitar la configuración predeterminada, fácil de adivinar, como la configuración 'privada' para la comunidad del servidor snmp.	Deshabilitar la cadena de comunidad SNMP predeterminada private
				`Router(config)#no snmp-server community {private}`
				Asegurarse de que no se muestre 'private':
				`Router# show snmp community`
				Estado Actual: _____

En el diseño de cada plantilla hardening, el tratamiento a estas brechas de seguridad presentadas en las configuraciones iniciales de los equipos de última milla, se agrupan por temas generales dando un orden, en el cual cada plantilla tiene sus particularidades según el fabricante del equipo.

Clasificación de Recomendaciones por fabricante

Fabricante	Tema
Cisco	Aseguramiento físico del dispositivo
	Reglas locales de autenticación, autorización y contabilidad (AAA)
	Reglas de Acceso
	Reglas de Contraseña
	Reglas SNMP
	Mejoras de inicio de sesión
	Reglas de servicio globales
	Reglas de Registro
	Reglas de NTP
	Reglas de loopback
	Reglas de enrutamiento
Juniper	Aseguramiento físico del dispositivo
	Firewall
	Interfaces
	Protocolos – BGP
	Protocolos – OSPF
	Protocolos – BFD
	SNMP
	Sistema - Contabilidad
	Sistema – Orden de Autenticación
	Sistema – Inicio de sesión
	Sistema – NTP
	Sistema – RADIUS / TACACS
	Sistema – Servicios
Cisco Meraki	Aseguramiento físico del dispositivo MX
	Aseguramiento de la conectividad WAN del dispositivo MX
	Configuración inicial Básica de la Organización del MX
	Aseguramiento de respaldo de la configuración MX

Fabricante	Tema
	Aseguramiento de la configuración Inicial del dispositivo MX
	Configuración Seguridad & SDWAN dispositivo MX
	Licenciamiento de los dispositivos MX

En estos grupos de remedición se desglosan más al detalle (Anexo 1).

Recomendaciones

Como resultado del levantamiento de información donde se identificaron las brechas de seguridad que son detonantes de las amenazas de seguridad, se basaron las recomendaciones en las buenas prácticas para su remediación. Estas recomendaciones se encuentran plasmadas en los diseños de las plantillas de hardening, que incluyen el paso a paso para tener en cuenta por parte de la compañía de telecomunicaciones para salvaguardar integridad, confidencialidad y disponibilidad de los equipos de última milla, donde se brindan las siguientes recomendaciones:

- Por parte de las áreas involucradas, técnicas y operativas en la compañía de telecomunicaciones, la implementación de las plantillas de hardening, diseñadas para los equipos de última milla de los fabricantes Cisco, Juniper y Meraki (Anexo 1) ya que estas están diseñadas para remediar la mayoría de las brechas de seguridad que tienen estos equipos con las recomendaciones más detalladas a nivel técnico, proporcionando un mayor aseguramiento y control sobre las configuraciones estándar iniciales que se aplican cuando se colocan en producción.

- A las áreas operativas mantener capacitaciones periódicas a sus empleados, tanto nuevos como antiguos, en relación con las prácticas de seguridad realizadas mediante las plantillas de hardening, ya que los empleados al tener siempre claras estas prácticas es posible que, en las futuras implementaciones de los equipos, se tenga un grado mayor de cumplimiento y eficacia en torno a la seguridad de los equipos.

- Tener identificados y documentados en detalle los dispositivos de última milla que van a instalarse en los clientes finales, por marca y modelo, serial, fin de soporte, versión de firmware, EoL (Tiempo de vida útil), con el fin de tener una base de datos que proporcione de manera proactiva alertamientos sobre esta información, como por ejemplo expiración de soporte.

- Tener plenamente identificadas y documentadas las brechas de seguridad presentes en los equipos que son susceptibles de ser aprovechadas por las amenazas generales y que podrían comprometer su seguridad.

- Dar a conocer públicamente las políticas al interior de la organización que fomenten la implementación de las buenas prácticas de seguridad en los equipos de última milla. Dichas políticas deben ser aplicadas por las áreas involucradas en la entrega y puesta en marcha de los equipos al cliente final.

- Es necesario que las áreas involucradas luego de la implementación de estos dispositivos realicen un barrido periódico del estado de su seguridad, y debe estar orientado a mantener la integridad, confidencialidad y disponibilidad.

- A nivel contractual, la organización debe establecer determinadas cláusulas con los clientes con los cuales tiene una administración compartida de los equipos instalados, para que éstos también realicen internamente y de manera periódica una revisión de estos dispositivos. La organización puede sugerirle a sus clientes que adopten las plantillas de hardening aquí realizadas como posibles herramientas con las cuales podría contar para dar cumplimiento a las cláusulas.

- Todos los dispositivos en la red de la compañía que estén en producción deben actualizarse y ejecutar la versión más actual de software y firmware recomendada por el fabricante y aplicar con periodicidad los parches de software en los equipos que tengan un contrato de soporte con la compañía. Estos contratos a su vez también deben actualizarse con regularidad.

- La compañía de telecomunicaciones debe asegurarse que los dispositivos EoL (End of Life) nunca deben usarse en redes de producción, ya que, para estos equipos, el fabricante ha anunciado que ha finalizado su vida útil y no ofrece parches, correcciones de errores o correcciones para vulnerabilidades de seguridad, representando un riesgo significativo para la seguridad de la organización.

- Realizar copias de seguridad periódicas, ya que a pesar de que los equipos son susceptibles a cambios originados por ya sea por solicitudes de parte de los clientes, fallas de hardware o ataques a la red, se ha evidenciado que estas copias no se realizan con la periodicidad deseada y su almacenamiento no es el correcto para que siempre estén disponibles.

- Los dispositivos deben tener instalada la máxima memoria RAM soportada, ya que, al tener la mayor cantidad de RAM disponible, ayuda a mitigar los ataques de denegación de servicios que agotan los recursos de memoria, aumentando la capacidad del dispositivo para sobrevivir a estos tipos de ataque, a su vez que aumenta su performance.

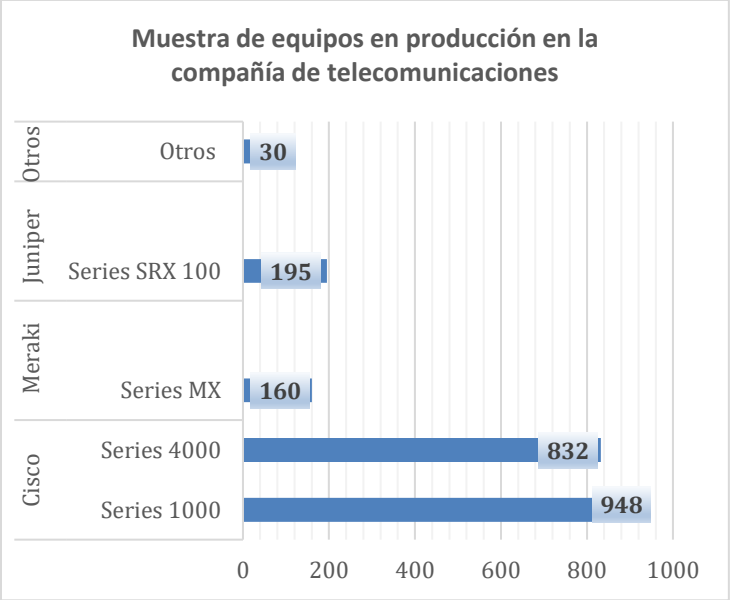
- Llevar un control de los registros y eventos generados en los dispositivos en los cuales no está habilitado, para así monitorearlos periódicamente y encontrar cambios y/o cualquier tipo de actividad que se considere sospechosa. Así mismo, se recomienda realizar un endurecimiento de los controles ya existentes.

- En la organización todo dispositivo que haya finalizado su servicio debe tener un adecuado proceso de retiro, en caso de que haya finalizado su vida útil o en el caso en el que cliente haya finalizado un contrato de servicio. Esto implica poner el sistema retirado en cero, devolviéndolo a su estado original predeterminado de fábrica, eliminando toda configuración presente del cliente, copias de seguridad almacenadas, etc. Esto con el fin de evitar que atacantes obtengan datos confidenciales mediante la adquisición de dichos equipos de red retirados, bien sea, a través del reciclaje o ventas de equipos usados en línea.

- Sin embargo, las buenas prácticas aquí indicadas, de nada sirven si el eslabón más débil que es el ser humano no comprende su importancia. es necesario que tengan claras las políticas qué con periodicidad realiza la compañía, mediante capacitaciones y que teniendo esto claro, es posible que, en las futuras implementaciones, las prácticas aquí recomendadas tengan un grado mayor de cumplimiento y eficacia.

11. Resultados

Como primer resultado del levantamiento de información, obtuvimos la visibilidad de una muestra de los equipos de última milla que están en producción por parte de la compañía de telecomunicaciones y que provee a sus clientes, con un total de 2165 equipos, de los cuales tienen participación los fabricantes Cisco con un 82% con sus series Cisco ISR 1000 e ISR 4000, Juniper con un 9% con las series SRX100 y la nueva tecnología en crecimiento SDWAN Cisco Meraki con un 7% la serie MX, logrando enfocar el diseño de las plantillas de hardening a tres, una para cada fabricante de modelos de equipos de última milla.



Por medio de este levantamiento de información también se pudo determinar los modelos de las series en los cuales enfocar las buenas prácticas, obteniendo un adecuado desarrollo de las plantillas hardening. Luego de un análisis realizado a las configuraciones iniciales de los equipos en producción, encontramos un aproximado de 32 brechas de seguridad que podrían ser aprovechadas por actores malintencionados, clasificándolas de acuerdo con la marca y modelo que podrían afectar.

Con base en las buenas prácticas mencionadas en el sitio web CIS Workbech (tanto para Cisco IOS como para Juniper) y el sitio web *General MX Best Practices Meraki*, identificamos las remediaciones para suplir estas brechas anteriormente identificadas, agrupándolas en un diseño de hardening, en el cual se expone los parámetros que se aconsejan cambiar y un procedimiento

detallado paso a paso para su remediación. (Anexo 1)

Como resultado de las remediaciones realizadas a las brechas de seguridad documentadas en las plantillas hardening, aconsejamos las siguientes recomendaciones a tener en cuenta por parte de la compañía de telecomunicaciones para salvaguardar integridad, confidencialidad y disponibilidad de los equipos de última milla:

- Implementar a cabalidad de las plantillas de hardening.
- Realizar capacitaciones periódicas enfocadas a las buenas prácticas de seguridad realizadas con las plantillas de hardening.
- Aseguramiento físico del sitio de instalación del equipo.
- Aseguramiento del entorno físico de instalación del equipo.
- Identificar y documentar en detalle de los dispositivos de última milla en producción.
- Identificar y documentar las brechas de seguridad presentes en los equipos.
- Fomentar al interior de la organización, la implementación de las buenas prácticas de seguridad.
- Revisar periódicamente el estado de la seguridad de los equipos tanto por parte de las áreas involucradas, como por parte del cliente.
- Actualizar periódicamente el software de los equipos.
- Evitar el uso de equipos que están por fuera de su vida útil.
- Realizar copias de seguridad periódicas y garantizar su disponibilidad.
- Contar con un adecuado proceso de retiro de los equipos que hayan finalizado su servicio o ya no cuenten con soporte por parte del fabricante.

12. Discusión

Analizando los resultados obtenidos de la muestra que se tomó en la región Colombia de los equipos de última milla de la compañía de telecomunicaciones, se logra el direccionamiento para enfocar los esfuerzos en el diseño de las plantillas de hardening, consiguiendo de manera porcentual la cantidad de equipos que se tienen por fabricante y series de modelo, ayudando a poder identificar las brechas de seguridad con más granularidad e incluso algunas pudiéndose extrapolar entre los modelos, ya que estos equipos independientemente de su marca tienen el mismo objetivo en la funcionalidad de los servicios que prestan.

Con la identificación de los equipos que tienen mayor participación en la instalación de los clientes finales se logra diseñar las plantillas de hardening en tres grupos de manera estandarizada, lo que hacen que sea más fácil de aplicar ya que pueden llegar a comprender una gran variedad de equipos de una misma serie por cada fabricante, determinado por la última versión de los sistemas operativos con los que estos funcionan.

Estas plantillas de hardening también tienen como resultado un gran detalle en las remediaciones de las brechas de seguridad que se identificaron en cada fabricante; su implementación es muy fácil de aplicar por parte del personal del área operativa de la compañía, ya que estos tienen el conocimiento necesario para la intervención de la configuración de los equipos, también la plantilla al generar una estandarización de las configuraciones optimiza los tiempos en la operación en cuanto la implementación inicial y ante un incidente la acción de recuperación del servicio es mucho más rápida.

Colocamos a disposición de la compañía de telecomunicaciones las siguientes recomendaciones

que deben ser aplicadas para asegurar exitosamente la integridad, confidencialidad y disponibilidad de la información en los equipos de última milla entregados al cliente.

Es importante destacar la importancia de deshabilitar los servicios inseguros, contar con adecuadas políticas de acceso a los equipos, y tener buenos mecanismos para realizar copias de respaldo de las configuraciones de los equipos, ya que de no tener esto en cuenta, podrían convertirse en factores de riesgo que pudiesen potencializar un ataque. Estos factores representan un riesgo organizacional a nivel interno, ya que los colaboradores de las áreas operativas tienen pleno conocimiento de su existencia. Aunque la mayor parte de los empleados conocen y cumplen las políticas de seguridad, cabe destacar que en toda organización puede haber los llamados insiders que son empleados actuales o exempleados, socios comerciales contratistas y/o proveedores que no sigan estos lineamientos, y representen una probabilidad muy grande de ser quienes exploten o dejen expuestas las debilidades existentes de forma malintencionada o no intencionada, causando graves perjuicios a la organización.

Para la organización, especialmente para las áreas operativas, consideramos que es muy importante establecer mecanismos que faciliten la utilización de las plantillas de hardening, bien sea a través de procesos o políticas internas entre áreas. Es necesario divulgar las buenas recomendaciones de seguridad relacionadas en estas plantillas con todas las áreas involucradas, del nivel más bajo en la organización al nivel más alto, de manera que se pueda comprender la importancia de un aseguramiento efectivo de los activos de la compañía frente a las diversas amenazas existentes. Consideramos necesario que, dentro de las tareas que desempeñan las áreas en el momento de realizar la instalación y entrega de los servicios a los clientes, la aplicación de estas plantillas sea parte de las labores cotidianas.

Precisamente mediante las plantillas de hardening buscamos brindar a la compañía, aparte de una mayor seguridad un mayor performance en los equipos, teniendo en cuenta las recomendaciones más actuales por parte de los expertos. Consideramos que, mediante la implementación efectiva y periódica de estas plantillas, las áreas operativas podrían darle un valor agregado a la compañía, haciéndola competitiva frente a otras compañías en cuestión de seguridad de los equipos de última milla, reduciendo costos de operación al disminuir los riesgos existentes en las configuraciones.

13. Conclusiones

La aplicación efectiva de las remediaciones documentadas en las plantillas de hardening mejora sustancialmente el aseguramiento de la infraestructura tecnología de las soluciones de última milla que ofrece la compañía. Esto, sumado a la implementación de estrictas políticas de usuarios, la capacitación periódica del personal técnico que implementa estas soluciones, y la adecuada adopción de estas buenas prácticas en la operación diaria, blinda a la organización ante las posibles amenazas que pudiesen presentarse, a la vez que les genera una buena reputación dentro del nicho de las telecomunicaciones. Por lo que podemos ver que el efecto que brinda este proyecto resulta ser muy beneficioso.

Del proyecto realizado, pudimos determinar que la compañía de telecomunicaciones ha realizado renovaciones tecnológicas en el último año. Esto lo pudimos determinar mediante la obtención de la información de los equipos que la compañía entrega a sus clientes, los cuales son modelos de última tecnología como lo son los enrutadores Cisco Series 1000, Así mismo, la compañía está apuntando a nuevas tecnologías como lo son las SD-WAN de Cisco Meraki.

Sin embargo, es necesario que la compañía conforme va progresando en sus tecnologías, paralelamente trabaje en el tema de su seguridad, ya que los equipos nuevos presentan brechas de seguridad que hay que solucionar antes de que estos salgan a producción.

Contrastando lo anterior, también pudimos determinar que la compañía provee servicios a sus clientes a través de enrutadores que ya finalizaron su vida útil, ya que en algunos modelos el fabricante no brinda soporte, y su utilización constituye un riesgo empresarial.

Se ha logrado dar visibilidad en que la seguridad en los equipos de última milla es de suma importancia, ya que son unos de los puntos más sensibles en las comunicaciones de una organización ante una amenaza si esta no ha sido debidamente identificada para su remediación, ya que lo daños a la compañía pueden impactar enormemente de manera negativa.

Pudimos concluir que las recomendaciones aquí planteadas teniendo como base las plantillas de hardening aplicadas hacia los equipos de última milla, son innovadoras y se pueden extender hacia otros proveedores de última milla que requieran aplican controles de seguridad en sus equipos.

14. Documentación de Referencia

1. TANLI, Ilker; KOLCALAR, Turgut. Deception Techniques, Methods, Honeypots, Honeynets and Usage. MontClair. Inglaterra: jun, 2017. 10 p.
2. STOLL, Cliff. Op. cit., p. 27.
3. BALTAZAR, J. (2011). Diseño e implementación de un esquema de seguridad perimetral. Para redes de datos caso práctico: dirección general del colegio ciencias y humanidades. 2016, de UNAM - México Disponible en: http://132.248.9.195/ptb2011/mayo/0669103/0669103_A1.pdf
4. SANCHEZ, O. (2011). Desarrollo de una guía para selección y endurecimiento (hardening) de sistemas operativos para un centro de datos. 2016, de IPN –México. Disponible en: http://tesis.ipn.mx/jspui/handle/123456789/8466
5. ROBAYO, J. (2015-01-04). Aseguramiento de los sistemas computacionales de la empresa Sitiosdima.net. Disponible en: http://hdl.handle.net/10596/3818
6. Fache, J. (2016). Estudio sobre la aplicación de hardening para mejorar la seguridad Informática en el centro técnico laboral de Tunjacotel
7. Morales, C. F. (2018). repositorio.ug.edu.ec. Obtenido de http://repositorio.ug.edu.ec/
8.https://2secure.co/wp-content/uploads/2017/06/Giotto-hardening-tool-2.pdf
9.https://www.cisco.com/c/en/us/products/routers/1000-series-integrated-services-routers-isr/index.html
10. https://www.cisco.com/c/dam/global/es_es/assets/pdf/en_06_4k_architecture_wp_pte_cte_es.pdf)
11. https://www.networkscreen.com/SRX100.asp
12. https://meraki.cisco.com/es-co/
13. https://meraki.cisco.com/lib/pdf/meraki_datasheet_mx_es.pdf
20. https://downloads.cisecurity.org/#/
21.https://repository.ucatolica.edu.co/bitstream/10983/25732/3/Anexo%20A-Gu%2B%C2%A1a%20de%20Hardening.pdf
22. https://www.inesem.es/revistadigital/gestion-integrada/amenazas-seguridad-fisica-sistemas-de-informacion/

15. Anexos

Anexo 1

(Carpeta de proyecto) Plantilla Hardening - SDWAN Meraki

(Carpeta de proyecto) Plantilla Hardening - CISCO IOS 17

(Carpeta de proyecto) Plantilla Hardening - Juniper OS

Anexo 2

(Carpeta de proyecto) Plantilla Formato Hardening