CONSULTORÍA DE SEGURIDAD PARA EL ANÁLISIS Y REMEDIACIÓN DE VULNERABILIDADES

Michael Stiven Lopez Amaya, Jeisson Joya Duitama, John Jaime Ruiz Guzmán, Hernán Alonso Ruiz Aguilar, Wilmar Amado Duarte

Especialización en Seguridad Informática, Fundación Universitaria Compensar

Propuesta de Consultoría

Miguel Ricardo Pérez Pereira

27 de mayo de 2023

Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional.

Consultoría de Seguridad para Análisis y Remediación de Vulnerabilidades

Michael Stiven Lopez Amaya
Jeisson Joya Duitama
John Jaime Ruiz Guzmán
Hernán Alonso Ruiz Aguilar
Wilmar Amado Duarte

Trabajo de grado presentado como requisito parcial para optar al título de:

Especialista en Seguridad Informática

Director (a):

Miguel Ricardo Perez Pereira

Fundación Universitaria Compensar

Facultad de Ingeniería, Especialización en Seguridad Informática

Bogotá, Colombia

2023

Resumen

El presente trabajo de titulación tiene como objetivo apoyar a las MiPymes en temas de ciberseguridad asociados a riesgos y en especial aplicar dichos conocimientos a la empresa Cable Fibra Plus, ya que dicha empresa ha manifestado que en los últimos meses han sido víctimas de varios incidentes de seguridad a causa de la debilidad de sus sistemas informáticos y a la falta de un adecuado tratamiento de las vulnerabilidades asociadas a su infraestructura con Windows Server, lo que ha derivado en indisponibilidad de sus servicios internos. Por lo anteriormente expuesto y para poder cumplir con los objetivos de minimización de riesgos se debe implementar una consultoría que abarque el estudio completo del contexto de la organización y de sus activos de información, esto se debe realizar a través de la identificación de riesgos que permita minimizar el impacto de los procesos internos que se manejan, teniendo en cuenta una serie de análisis y de consideraciones técnicas que permitan remediar las vulnerabilidades que tengan sus servidores, con el fin de evitar que dichas debilidades sean aprovechadas por los ciberdelincuentes o que los servicios sean intervenidos para denegarse.

Este proceso de remediación abarca una serie de recomendaciones técnicas y de herramientas que permitirán asegurar los sistemas y los aplicativos que se encuentran alojados en ellos, además de poder generar una metodología que le permitan a la organización tener una base técnica para poder actuar de manera efectiva ante cualquier ataque o riesgo nuevo que se presente sobre su infraestructura.

Palabras clave: Ciberseguridad, Remediación, Riesgos, Vulnerabilidades, Infraestructura, hacktivistas.

Abstract

The objective of this graduation project is to support SMEs in cybersecurity matters associated with risks, specifically applying this knowledge to the company Cable Fibra Plus. The company has reported being a victim of several security incidents in recent months due to the weakness of its computer systems and the lack of adequate treatment of vulnerabilities associated with its Windows Server infrastructure. This has resulted in internal service unavailability. To achieve the risk minimization objectives, it is necessary to implement a consultancy that encompasses a comprehensive study of the organization's context and its information assets. This should be done through risk identification to minimize the impact on internal processes, considering various analyses and technical considerations to remediate vulnerabilities on their servers. The goal is to prevent cybercriminals from exploiting these weaknesses or interfering with services.

This remediation process includes a set of technical recommendations and tools to ensure the security of systems and the applications hosted on them. Additionally, it aims to establish a methodology that provides the organization with a technical foundation to effectively respond to any new attack or risk that may arise against its infrastructure.

Keywords: Cybersecurity, Remediation, Risk, Vulnerability, Infrastructure, hacktivist.

Contenido

RESUMEN III

INTRODUCCIÓN 1

ANTECEDENTES Y JUSTIFICACIÓN 1
FORMULACIÓN DEL PROBLEMA 4
OBJETIVO GENERAL 5
Objetivos Específicos 5
ALCANCES Y LIMITACIONES 5

1. MARCO TEÓRICO 7

1.1 VULNERABILIDADES 8
1.2 REMEDIACIÓN 9

2. DISEÑO METODOLÓGICO 18

3. RESULTADOS 27

4. DISCUSIÓN 28

5. CONCLUSIONES Y RECOMENDACIONES 31

5.1 CONCLUSIONES 31
5.2 RECOMENDACIONES 32

BIBLIOGRAFÍA 33

Introducción

En la actualidad, con el auge del uso de las tecnologías para la automatización de procesos y servicios que se ofrecen a través de los diferentes canales de comunicación, las empresas por lo general y en particular las dedicadas a proveer servicios de internet tienen la necesidad de robustecer sus sistemas de seguridad, esto se logra entre otras cosas adoptando buenas prácticas en temas de ciberseguridad y, adicionalmente, mitigando las vulnerabilidades que tienen en su infraestructura de servidores. En esta propuesta se tiene como objetivo plantear una consultoría de seguridad enfocada en el análisis y remediación de vulnerabilidades sobre los servidores Windows de la empresa Cable fibra Plus, dicha propuesta de consultoría tiene en cuenta tres objetivos claros que son: proponer la metodología de trabajo, plantear el proceso de análisis y remediación de vulnerabilidades y por ultimo sugerir el método y la herramienta de trabajo para este fin, bajo una metodología previamente establecida que permitirá identificar, evaluar y mitigar las vulnerabilidades halladas, esto se hace después de escoger una herramienta de escaneo de vulnerabilidades para tal fin teniendo en cuenta las necesidades del negocio, como son: el contexto de la organización, los activos y la importancia que estos tengan en la operación, para poder gestionar de manera eficaz aquellos riesgos que estos tengan y mejorar la seguridad de la infraestructura.

Antecedentes y Justificación

Antecedentes

Existen innumerables ejemplos y antecedentes sobre la remediación de vulnerabilidades en las compañías, uno de los primeros proyectos que debemos citar sobre remediación de vulnerabilidades se ubica en Bogotá, Colombia y fue realizado por la Universidad Nacional Abierta y a Distancia para la empresa NOSTRADAMUS S.A.S donde los puntos principales del proyecto son:

- Basados en la metodología de la norma ISO27001:2013 identificaron todos los activos de la compañía y a partir de esta generaron el análisis de riesgo.
- Con la metodología definida realizaron un análisis para determinar el nivel de madurez del SGSI de esta compañía, identificando su estructura y descripción del proceso de aplicación con alcance a la infraestructura crítica.
- Se aplica Hacking Ético a la infraestructura en ambientes controlados con servidores virtualizados y el uso de S.O de auditorías como Kali Linux, esto desarrollado por un equipo de pruebas de penetración

El segundo proyecto se ubica en Bogotá, Colombia y fue realizado por la Universidad Piloto De Colombia para una entidad bancaria donde se propone una metodología para identificar y remediar las vulnerabilidades en la infraestructura, los principales puntos a tomar fueron los siguientes:

- Realizaron la clasificación de las vulnerabilidades detectadas y reportadas de acuerdo con su criticidad e impacto.
- Diseñaron un plan de remediación para las vulnerabilidades críticas que fueron reportadas con la ejecución de pruebas de intrusión.
- Definieron un control técnico a implementar las remediaciones y mitiga los riesgos asociados a las vulnerabilidades críticas.
- Definieron una metodología especifica que permitió el tratamiento y remediación de las vulnerabilidades críticas detectadas y/o explotadas en la prueba de intrusión realizada con fecha de octubre del 2016.

A nivel internacional la universidad UOC de Cataluña, España desarrolló un control y análisis de configuraciones de seguridad y vulnerabilidades para servidores empresariales donde implementó el protocolo SCAP (Security Content Automation Protocol) sus puntos principales fueron los siguientes:

- Investigación del protocolo SCAP y las soluciones que el mercado ofrece para la seguridad en servidores.

- Buscaron repositorios con las configuraciones SCAP para seleccionar ficheros (XCCDF) para configurar políticas de seguridad.
- Validaron las configuraciones de seguridad de seguridad con las herramientas Nessus y OpenScap.

En síntesis, con los antecedentes citados anteriormente podemos identificar un marco de referencia de los análisis y remediaciones que se han realizado en diferentes core de negocio y resalta la importancia la ejecución de estos análisis para ejecución de las remediaciones que haya a lugar.

Justificación

Con la masificación de los sistemas informáticos y la relevancia que estos tienen para la optimización de los procesos y servicios que ofrecen las compañías, es importante poder asegurar los activos de información que hacen parte del Core de negocio y que representan la mayoría de los ingresos que estas tienen. No ajenos a esta realidad, los ciberataques constituyen uno de los riesgos más frecuentes debido a la sofisticación de las formas en las que se acceden a estos sistemas de manera ilegal, por lo que es necesario contar con medidas preventivas de seguridad para proteger dichos activos, en ese sentido, tener un proceso robusto de identificación y remediación de vulnerabilidades es una necesidad donde se priorizan las debilidades que tienen estos sistemas para así realizar su debida gestión, lo que nos permite poder actuar de manera efectiva para garantizar su protección.

En el presente documento se plantea una propuesta metodológica que pretende añadir este proceso de seguridad para la empresa Cable Fibra Plus, donde la priorización de la gestión de vulnerabilidades que tiene su infraestructura interna es fundamental para evitar la interrupción de los procesos internos y así mismo, los servicios que se publican a través de estos, generando una propuesta de valor donde el foco principal es la gestión de la seguridad, minimizando el tiempo dedicado a remediar las vulnerabilidades que representan un alto riesgo para los activos de información. De esta manera se logra optimizar los recursos humanos y tecnológicos, lo que permite en ultimas reducir costos y mejorar la postura de

seguridad que tiene la empresa junto con la exposición de la infraestructura a un posible ciberataque.

Formulación del Problema

La empresa Cable Fibra Plus es un proveedor de servicios de Internet (ISP, por sus siglas en inglés de Internet Service Provider) que tiene una trayectoria de dos años en el mercado de las telecomunicaciones, cuenta con una infraestructura interna compuesta por servidores Windows y estaciones de trabajo que garantiza el desarrollo de sus procesos. Esto con el fin de mejorar la seguridad de su infraestructura interna la cual repercute directamente en la disponibilidad de los servicios que se les da a las diferentes áreas, teniendo en cuenta que, si se produce un incidente de seguridad o una interrupción de los sistemas, Cable Fibra corre el riesgo de sufrir pérdidas financieras y de reputación.
La empresa de telecomunicaciones Cable Fibra Plus tiene una infraestructura de servidores Windows que se utiliza para proporcionar servicios a sus clientes, incluidos servicios de correo electrónico, alojamiento de sitios web y almacenamiento en la nube. La empresa ha notado un aumento en los ataques cibernéticos a su infraestructura en los últimos meses, lo que ha generado preocupación en la dirección de la empresa.

El problema que se presenta en la infraestructura interna de una empresa es la falta de medidas de seguridad y controles adecuados para proteger los datos y sistemas críticos de la empresa. Este problema es muy común en las empresas de hoy en día, ya que la mayoría de ellas dependen en gran medida de la tecnología y las aplicaciones para realizar sus operaciones diarias. El equipo de seguridad de la empresa ha identificado que los servidores Windows de la empresa no cuentan con las medidas de seguridad adecuadas para protegerse de los ataques cibernéticos, lo que los convierte en un objetivo fácil para los ciberdelincuentes. La empresa también ha identificado que hay vulnerabilidades en algunos de sus sistemas que podrían ser explotados por los atacantes.

Por consiguiente, la pregunta de investigación que nos atañe es la siguiente: ¿es posible con un análisis de vulnerabilidades y remediación evitar y mitigar este tipo de vulnerabilidades en la red de servidores de la empresa? El objetivo de esta propuesta de consultoría de seguridad de servidores Windows es ayudar a la empresa, a mejorar la seguridad de su infraestructura de servidores Windows y reducir el riesgo de ataques cibernéticos. Para

lograr este objetivo, se propone una evaluación de la infraestructura actual, identificando las vulnerabilidades y debilidades existentes. A partir de esta evaluación, se propondrán soluciones y se implementarán medidas de seguridad para reducir los riesgos y mejorar la seguridad general de los servidores Windows de la empresa.

Objetivo General

Plantear una consultoría para el análisis y remediación de vulnerabilidades en los servidores de la empresa Cable fibra Plus, con la finalidad de fortalecer la seguridad de la infraestructura de servidores Windows.

Objetivos Específicos

- Proponer la metodología para la identificación de las vulnerabilidades en la infraestructura de servidores Windows de la empresa Cablefibra Plus.

- Plantear el proceso de análisis y evaluación de los riesgos asociados a cada vulnerabilidad identificada.

- Sugerir el método y la herramienta de remediación acorde a las vulnerabilidades identificadas en los servidores Windows.

Alcances y Limitaciones

En este documento se propone estudiar tres de las herramientas más implementadas en el mercado para el análisis de vulnerabilidades y a partir de esta evaluación, seleccionar la que mejor cumpla con las necesidades técnicas y económicas de la empresa. Una vez seleccionada e implementada y con base en los resultados generados, se recomendará priorizar la remediación en función de la criticidad de estos resultados. Lo que garantizará la efectividad de las remediaciones implementadas, al concentrar las acciones en aquellos servidores que presentan una mayor lista de vulnerabilidades.

1. Marco teórico

La vulnerabilidad es una debilidad o error en un sistema o software, las vulnerabilidades existen, no se desarrollan, generalmente son aprovechadas, por un atacante para exponer la seguridad del sistema, corromper datos o acceder a información privada. La vulnerabilidad puede tener una característica premeditada o una falencia involuntaria en el diseño, ejecución o construcción de un sistema, red o software, la vulnerabilidad, es una debilidad que podría ser explotada, por actores maliciosos como grupos del crimen organizado, hacktivistas, aficionados o grupos terroristas que usan el ciberespacio con el objetivo de afectar negativamente, a los individuos como las corporaciones.
(Sánchez-Sánchez et al., 2021)(Peñafiel Lucy, 2021)(Sánchez-Sánchez et al., 2021)(NEXNET, n.d.)

Una falla informática es un problema que ya está afectando el funcionamiento del sistema o software, este error o defecto provoca que el servicio tenga interrupciones o se bloquee, incluso se tengan perdidas de datos de estos.

Debemos ser conscientes que una falla o error informático da como resultados fisuras o puertas abiertas que consideramos como vulnerabilidades, por ende, se debe solucionar en el menor tiempo posible para mitigar los riesgos de seguridad, por esta razón, es necesario que a los sistemas informáticos se les realicen análisis de vulnerabilidades, para identificar y remediar antes que sean explotadas por un atacante. (Sánchez-Sánchez et al., 2021)(Yan et al., 2019)(AboElFotoh et al., 2005)

Un análisis de vulnerabilidad informático es un proceso sistemático y exhaustivo de evaluación de los sistemas informáticos, redes y aplicaciones para identificar debilidades y vulnerabilidades en su seguridad. El objetivo del análisis es determinar el grado de riesgo que representa una posible explotación de las vulnerabilidades identificadas y ayudar a los

administradores de sistemas y a los responsables de la seguridad informática a tomar medidas para mitigar los riesgos. (Kurniawan, 2017)(Marcillo Parrales et al., 2020)(Gómez, 2014)

Durante un análisis de vulnerabilidad, se realizan pruebas en el sistema para detectar posibles debilidades y se evalúa el nivel de amenaza que representa cada una de ellas. Esto incluye la revisión de los sistemas operativos, aplicaciones, configuraciones de red, políticas de seguridad, entre otros.

Es importante destacar que el análisis de vulnerabilidad es un proceso continuo y en constante evolución, ya que los sistemas y las amenazas cambian constantemente. Por lo tanto, es fundamental que las organizaciones realicen análisis de vulnerabilidad de manera regular para garantizar la seguridad de sus sistemas informáticos.

1.1 Vulnerabilidades

Existen muchas vulnerabilidades informáticas que pueden ser explotadas por los ciberdelincuentes, pero algunas de las más frecuentes incluyen:

- Fallos en la configuración de seguridad: Las configuraciones incorrectas pueden dejar los sistemas y redes vulnerables a ataques. Por ejemplo, utilizar contraseñas débiles, no cambiar las contraseñas predeterminadas, permitir el acceso remoto no seguro, entre otros.

- Fallos de software y sistemas operativos: Los programas y sistemas operativos pueden tener errores de programación y de seguridad, que pueden ser explotados por personal no autorizado para acceder a sistemas y datos sensibles.

- Fallos en las aplicaciones web: Las aplicaciones web pueden contener vulnerabilidades que permiten a los atacantes comprometer la seguridad del sitio web o acceder a bases de datos sensibles y denegar el acceso a información de las organizaciones a los usuarios.

- Phishing y suplantación de identidad: Los atacantes pueden enviar correos electrónicos o mensajes de texto engañosos para engañar a los usuarios y obtener información confidencial como contraseñas o información de cuenta bancaria o datos sensibles.

- Malware: El malware es un software malicioso diseñado para dañar los sistemas y robar información. Pueden entrar en los sistemas a través de correos electrónicos, descargas en línea y dispositivos USB infectados y entre los que podemos mencionar como: Ransomware, Spyware, gusanos, Adware, Troyanos, Bonets etc.

En el contexto local, entre enero y octubre de 2022, en Colombia se reportaron 54.121 denuncias por ciberataques, según cifras del Centro Cibernético de la Policía Nacional. Como ejemplo de estos ciberataques podemos mencionar algunas de las empresas que fueron hackeadas en Colombia durante el 2022, como fueron: EPM, EPS Sanitas, Salud Total, Invima, Universidad Piloto, Claro Colombia, Electricaribe, Viva Air, Famisanar, Corferias, OpenGroup SAS etc. Según Lumu Technologies, esto tuvo un incremento del 133% en el número de empresas atacadas por Ransomware, el cual consiste en secuestrar la información, y luego pedir un pago a las organizaciones para recuperar sus datos. (Alert,2021)Alert, A. (2021).

Es importante tener en cuenta que estas vulnerabilidades pueden variar dependiendo del tipo de sistema y tecnología utilizada, y es necesario realizar un análisis de vulnerabilidad para identificar y mitigar las amenazas específicas a cada sistema.

1.2 Remediación

La ciberseguridad es una preocupación creciente en el mundo de la tecnología, y la remediación es uno de los principales mecanismos de cualquier táctica de seguridad efectiva. Las soluciones de remediación en ciberseguridad son esenciales para proteger las redes y los sistemas informáticos de posibles amenazas y ataques.

la importancia de las medidas de una remediación son los diferentes tipos de soluciones, su implementación, las mejores prácticas para su selección y varias soluciones efectivas para diferentes tipos de ataques. La prevención es importante, pero siempre hay la existencia de un riesgo residual, o la posibilidad de que una amenaza pueda pasar desapercibida, en estas

situaciones la capacidad de responder y recuperarse rápidamente es crítica para minimizar el impacto y eliminar cualquier daño realizado a la víctima.

Para esto podemos implementar varios tipos de remediaciones disponibles, en los cuales podemos incluir la recuperación de datos sensibles de las compañías o usuarios, medidas y soluciones para la protección de la red, la eliminación de malware y la prevención de intrusiones. Cada una de estas soluciones se enfocarán en aspectos diferentes en la seguridad de la red y del sistema informático.

Recordemos que las soluciones preventivas se enfocan en evitar que las amenazas ingresen al sistema informático, mientras que las soluciones reactivas se enfocan en remediar los problemas después que han ocurrido, por esta razón se aconseja tener la combinación de las siguientes soluciones con el fin de tener un enfoque efectivo y equilibrado en la seguridad, como son algunas de las siguientes soluciones:

- Parches de seguridad: Los parches son actualizaciones de software que corrigen las vulnerabilidades conocidas y mejoran la seguridad del sistema. Es fundamental instalar los parches de seguridad tan pronto como estén disponibles para mitigar los riesgos.

- Configuraciones de seguridad: Es importante revisar y mejorar las configuraciones de seguridad en los sistemas y redes para reducir las vulnerabilidades. Esto incluye el uso de contraseñas seguras, deshabilitar servicios innecesarios, restringir el acceso de usuarios, entre otros.

- Pruebas de penetración: Las pruebas de penetración son evaluaciones simuladas de los sistemas y redes para identificar las vulnerabilidades y los puntos débiles. Estas pruebas pueden ayudar a identificar los riesgos y permiten tomar medidas preventivas.

- Actualizaciones de software: Es importante mantener el software actualizado para corregir las vulnerabilidades conocidas. A menudo, las nuevas versiones del software incluyen correcciones de seguridad que pueden reducir los riesgos de seguridad.

- Formación y concientización: Los usuarios son un eslabón importante y débil en la seguridad de los sistemas y redes, por lo que es importante proporcionar formación y

concientización sobre las buenas prácticas de seguridad informática y las amenazas comunes.

Las mejores prácticas para la selección de soluciones involucran la evaluación de las necesidades del COR de la empresa, la identificación más común, la selección de las herramientas o soluciones efectivas y confiables, sin olvidar el aspecto más importante y débil en esta cadena que es el usuario, con la finalidad que puedan trabajar de la mano con la nueva solución. (Dalziel & Caceres, 2014)(Van der Linden, 2019)(Deckard, 2005)(Karimipour et al., 2020)(Pelton & Singh, 2015)(Daimi et al., 2017)(Göbel & Dewald, 2011)

Las herramientas que se van a recomendar para esta propuesta de consultoría son las siguientes:

Nexpose

Es una herramienta que encuentra activos y explora en busca de vulnerabilidades dentro de contextos móviles, virtuales y físicos incluso en la nube de compañía, priorizando el riesgo en función de la explotabilidad de dichas vulnerabilidades, esta herramienta puede priorizar los parches de vulnerabilidades de forma regular de este modo permite a los administradores establecer alarmas de seguridad.

Esta herramienta incluye una función única de supervisión en tiempo real, que recopila todos los datos accesibles y los traduce en planes de acción. La avanzada función de análisis de Nexpose localiza y prioriza las vulnerabilidades que se explotan primero, por esta razón los encargados de la seguridad se ahorran el exceso de notificaciones de seguridad, una de las funciones es Liveboard, se aplica para sustituir los resultados de un panel estático por informes visuales y dinámicos, esto nos permite una mejor percepción de la información que nos presenta esta herramienta.

Rapid 7 ha lanzado una nueva herramienta para Nexpose llamada remediación workflow, que se utiliza para rastrear y gestionar a los empleados del SOC de la empresa, de igual forma analizar el progreso de la corrección de las vulnerabilidades.

Características de Nexpose más destacadas podemos mencionar las siguientes:

- Escaneo de la infraestructura de IT para detectar vulnerabilidades.
- Priorización de vulnerabilidades según la importancia y el riesgo asociado
- Generación de reportes detallados sobre las vulnerabilidades encontradas
- Integración con otras herramientas de ciberseguridad
- Gestión de políticas de seguridad
- Automatización de tareas de seguridad
- Actualización de base de datos de las vulnerabilidades

Por otro lado, Nexpose cuenta con una arquitectura distribuida que permite la escalabilidad y la disponibilidad de la herramienta, esta se compone de tres elementos principales: el motor de escaneo, el motor de análisis el cual procesa la información para detectar las vulnerabilidades y la consola de administración que es la interfaz de usuario para la gestión de la herramienta.

El funcionamiento de Nexpose se basa en la detección de vulnerabilidades en la infraestructura de IT, Para ello la herramienta realiza los escaneos de los sistemas y dispositivos de la organización, y realiza el análisis de la información recopilada para identificar las vulnerabilidades, después de detectar las vulnerabilidades las prioriza según el riesgo asociado y origina un reporte detallado de las mismas, permitiendo la automatización de tareas de seguridad para mejorar la eficacia y efectividad de la gestión de las vulnerabilidades.

Análisis y reportes de Nexpose

La generación de reportes detallados sobre las vulnerabilidades encontradas es otra de las funciones importantes de Nexpose, esto permite la generación de reportes personalizados, que pueden ser acondicionados a las necesidades de cada organización, los reportes incluye información detallada sobre las vulnerabilidades encontradas, la priorización de las mismas y además de esto las recomendaciones para su mitigación, estos reportes se pueden compartir exportándolos en diferentes formatos, como PDF o CSV, para facilitar su análisis, distribución y trabajo colaborativo.

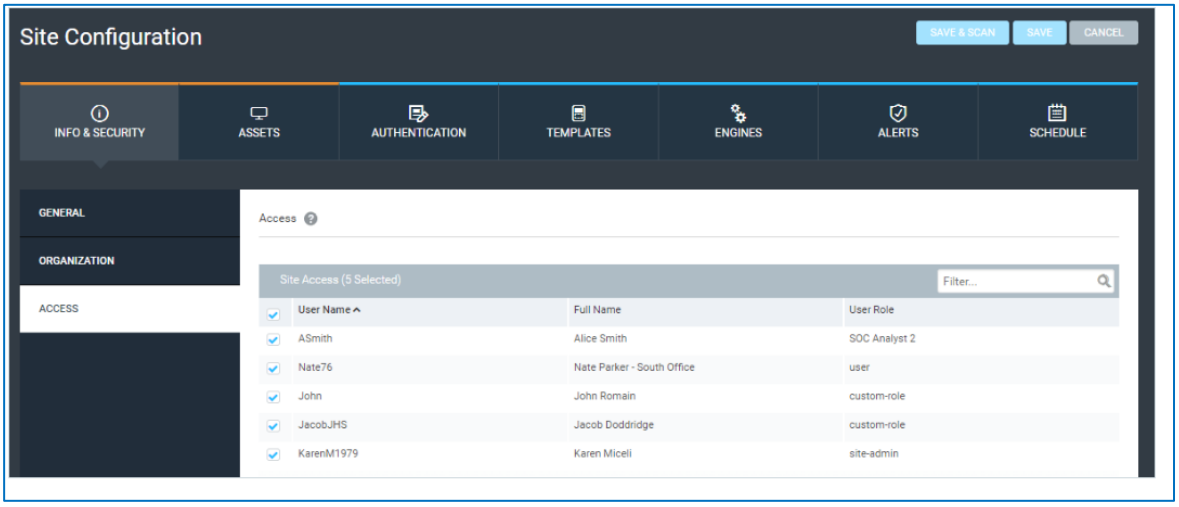


Figura 1 Configuración de acceso Nexpose

Integración con otras herramientas de ciberseguridad

Nexpose también permite la integración con otras herramientas de ciberseguridad lo que la convierte en una herramienta muy versátil, esta integración permite la automatización de tareas y mejora su eficiencia en la gestión de vulnerabilidades, por ende, la integración con otras herramientas permite la obtención de información más completa sobre la infraestructura de TI, lo que puede ser útil para la detención de las amenazas y la toma de decisiones en su remediación.

Automatización de tareas

La automatización de las tareas en Nexpose permite la mejora de la gestión de vulnerabilidades, permite la automatización de tareas como la programación de escaneos, la generación de reportes y la aplicación de parches de seguridad, la automatización de tareas permite la reducción del tiempo y los recursos necesarios para la gestión de vulnerabilidades.

Qualys

Es una plataforma de seguridad en la nube que se utiliza para la gestión de vulnerabilidades y el cumplimiento de políticas de seguridad en empresas de todos los tamaños. La herramienta ayuda a los equipos de seguridad a detectar y remediar vulnerabilidades en tiempo real y a proteger y mantener la integridad de la infraestructura de TI. Qualys proporciona una amplia

gama de herramientas de seguridad de red, como detección de amenazas, gestión de parches, evaluación de vulnerabilidades y cumplimiento de políticas. La herramienta Qualys también es muy escalable y puede adaptarse a los requisitos de seguridad de cualquier organización.

Qualys tiene varias funciones importantes que la hacen una herramienta útil en la lucha contra las amenazas cibernéticas. Entre ellas se incluyen:

- Escaneo de vulnerabilidades: Qualys realiza un escaneo completo de la red y los sistemas informáticos para identificar posibles vulnerabilidades y brechas de seguridad. Esto incluye análisis de puertos, servicios, sistemas operativos, aplicaciones y otros elementos de la red.

- Gestión de parches: Qualys ofrece una gestión automatizada de parches, lo que significa que puede ayudar a las empresas a identificar y usar parches de seguridad críticos en su red y sistemas informáticos.

- Cumplimiento de políticas: Qualys puede ayudar a las empresas a cumplir con los requisitos de cumplimiento de políticas de seguridad, como PCI DSS, HIPAA, GDPR, entre otras.

- Análisis de riesgos: Qualys proporciona una evaluación de riesgos que ayuda a las empresas a comprender la gravedad de los problemas de seguridad identificados. Esta evaluación de riesgos incluye información sobre la probabilidad de una brecha de seguridad, el impacto potencial en la empresa y las posibles consecuencias.

- Análisis de la postura de seguridad: Qualys ofrece una vista completa de la postura de seguridad de una empresa, lo que permite a los especialistas en ciberseguridad identificar y solucionar problemas de seguridad de manera eficiente. La integración de Qualys con otros sistemas de seguridad puede mejorar la eficacia de la gestión de vulnerabilidades y ayudar a las organizaciones a protegerse de los ataques cibernéticos.

- Creación de informes personalizados: Qualys permite a los especialistas en ciberseguridad crear informes personalizados que incluyen información detallada sobre las vulnerabilidades identificadas, la gravedad de los problemas y las recomendaciones para mitigarlos. Estos informes son muy útiles para presentar a la dirección y ayudarles a comprender el estado de seguridad de la empresa. (Cortés Santamaría, 2021)(Villora Divino, 2018)(Giménez Campos, 2020)

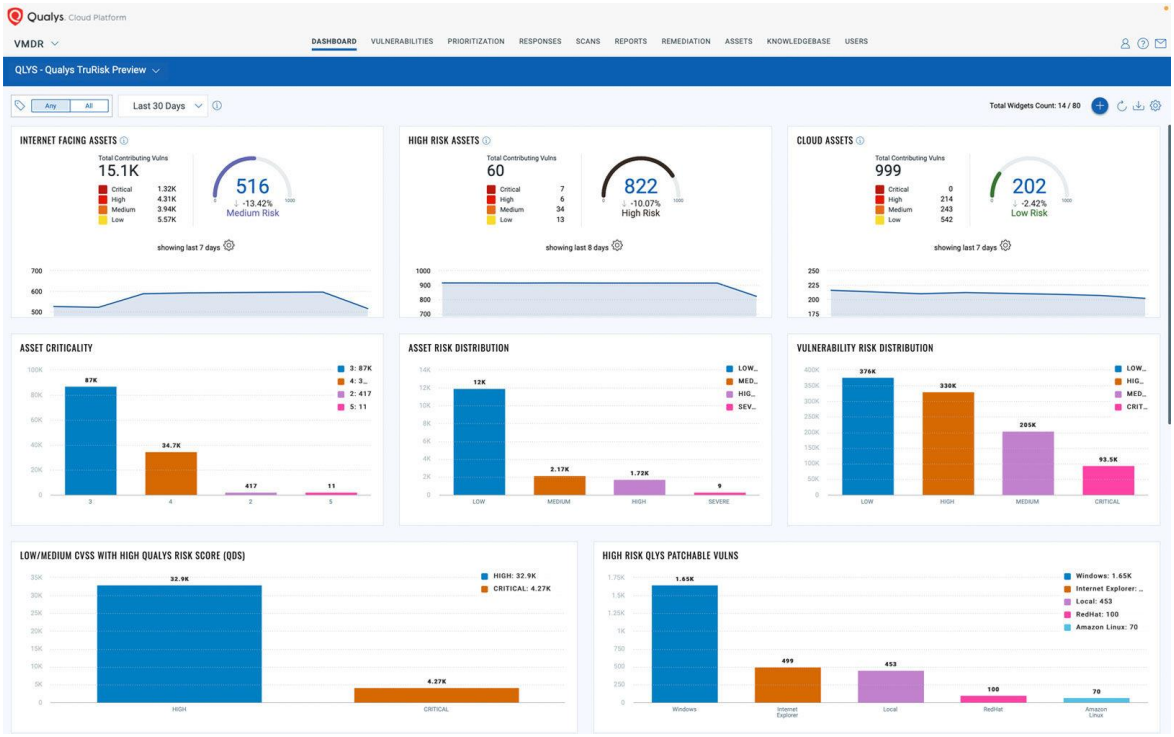


Figura 2 Dashboard vulnerabilidades (Guide, 2006)

- Algunas de las opciones que se pueden visualizar en la anterior figura barra del menú son las siguiente:
    - Dashboard: permite ver un resumen gráfico de varias variables, tal como vulnerabilidades por nivel de severidad, y por status.
    - Map: generación de mapas para descubrimiento de IP's en la red
    - Scan: ejecución de escaneos de vulnerabilidades y de cumplimiento de normas
    - Schedule: agendamiento de tareas y escaneos
    - Report: generación de reportes
    - Remediation: sistema de tickets de remediación
    - Asset Search: búsqueda de máquinas en base a parámetros como IP, sistema operativo, o servicios que esté corriendo
    - Risk Analisis: descubrimiento de forma rápida sobre los hosts en búsqueda de una vulnerabilidad en particular
    - Asset Groups: creación de grupos de activos

Nessus

Es una herramienta que en sus inicios era software libre, pero después fue adquirido por la empresa Tenable, convirtiéndose en una solución robusta en el mercado, para su utilización de forma gratuita es necesario registrarse en su sitio web para obtener la licencia, para utilizar la comercialmente o en el sector empresarial se debe comprar la licencia de pago, la versión Profesional provee los mismos Plugin que la versión Home, junto con otros módulos que permiten auditar los sistemas SCADA.

Esta herramienta nos permite también, escanear las vulnerabilidades de forma automatizada, identificación y priorización de vulnerabilidades, generación de informes, integración con otras herramientas, escaneos de credenciales.

Nessus es una herramienta de análisis de vulnerabilidades que permite a los administradores de seguridad identificar posibles debilidades en la red. Las funciones principales de Nessus incluyen la identificación de vulnerabilidades en los sistemas, la evaluación del riesgo asociado a estas vulnerabilidades, y la recomendación de soluciones para su corrección. Nessus también ayuda en la auditoría de cumplimiento con estándares de seguridad como PCI DSS, HIPAA y ISO 27001.

Características

Nessus cuenta con una amplia variedad de características para mejorar la eficacia de la protección cibernética. Por ejemplo, Nessus tiene una biblioteca con más de 100,000 plugins de vulnerabilidades que se actualiza regularmente. Nessus también ofrece escaneos de vulnerabilidades en la red, escaneos de credenciales, escaneos de aplicaciones web y escaneos de contenedores. Nessus también cuenta con una interfaz de usuario intuitiva y fácil de usar.

Escaneo de Vulnerabilidades

El escaneo de vulnerabilidades en Nessus comienza con la definición de un objetivo de escaneo. Este objetivo puede ser una dirección IP, un rango de direcciones IP o un nombre de host, escanea el objetivo utilizando una biblioteca de plugin de vulnerabilidades y genera un informe de resultados. Los plugin de Nessus identifican vulnerabilidades en el sistema y proporcionan información detallada sobre la vulnerabilidad, su riesgo asociado y las soluciones recomendadas.

El análisis de resultados se realiza con la interpretación y estadísticas de los informes, Nessus se integra con otras herramientas de seguridad cibernética para mejorar la eficacia de la protección cibernética. Por ejemplo, Nessus se integra con herramientas de gestión de parches y con sistemas de gestión de eventos y de información de seguridad (SIEM). La integración con SIEM permite a los administradores de seguridad automatizar la respuesta a eventos de seguridad y la gestión de vulnerabilidades

Automatización

Nessus ofrece numerosas API's que permiten a los administradores de seguridad automatizar tareas. Las API's de Nessus pueden utilizarse para crear políticas de escaneo, ejecutar escaneos, generar informes y gestionar vulnerabilidades. Las API's de Nessus también pueden integrarse con otras herramientas de seguridad cibernética, permitiendo una mayor automatización y eficiencia en la protección cibernética

Nessus ha sido utilizado en numerosos casos para prevenir ataques y mejorar la protección cibernética. Por ejemplo, Nessus fue utilizado para identificar y corregir una vulnerabilidad crítica en el software utilizado por el Departamento de Estado de EE. UU. Nessus también fue utilizado para identificar una vulnerabilidad en el sistema de votación electrónica de una ciudad en Alemania, lo que permitió la corrección antes de las elecciones. (Barinas et al., 2014; V.A.R.Barao et al., 2022)

Costos de Licenciamiento

El siguiente es un cuadro comparativo de costos de licenciamiento entre las tres herramientas propuesta a implementar:

Herramienta	Valor total Licencia anual	Servidores Cablefibra Plus	Activos	Total Licencia por año	Activos
Nessus	$ 32.500.000	8	48	$ 15.600.000	100
Nexpose Insight VM	$ 10.000.000			$ 4.800.000	100
Qualys	$ 35.000.000			$ 16.800.000	100

Tabla 1. Costos de licenciamiento para Cable Fibra Plus

2. Diseño Metodológico

La propuesta de consultoría está fundamentada en el modelo de investigación de acción, mediante el cual, haciendo un estudio de la problemática actual de la empresa, podemos desarrollar un modelo para la implementación de una solución práctica que permita mejorar la postura de seguridad de la empresa. La metodología previamente propuesta identifica todas aquellas vulnerabilidades que generan mayor riesgo e impacto sobre la infraestructura de Cable Fibra Plus. Para esto se debe identificar una serie de Variables que son: Identificación de vulnerabilidades críticas en servidores Windows, Minimización de riesgos de explotación y ocurrencia de una vulnerabilidad identificada.

2.1 Elección de herramienta

Para establecer una metodología que permita cumplir con los objetivos, lo primero es la identificación de las vulnerabilidades en la infraestructura de servidores, para lo cual se deben investigar las distintas herramientas que nos permitan realizar un escaneo efectivo sobre la infraestructura. Posteriormente se realiza una evaluación técnica de dichas herramientas, basándose en el cumplimiento de una serie de criterios. adicionalmente, y teniendo en cuenta el contexto de la empresa y de los procesos que manejan estos servidores, se puede tener un mayor nivel de certeza en cuanto a los hallazgos de las vulnerabilidades y la criticidad que éstas tengan sobre cada servidor o proceso.
A continuación, se analizarán las tres herramientas mencionadas anterior mente, dichas herramientas son:

Las tres herramientas tomadas como propuestas para la investigación y posterior evaluación son: Nexpose, Nessus y Qualys, las cuales se identifican o catalogan como las más populares en los últimos años debido al desarrollo y efectividad que han tenido en el área de la seguridad en cuanto a escaneos de vulnerabilidades se refiere.

La metodología propuesta define que estas herramientas deben ser instaladas en los servidores de la compañía con el fin de realizar el proceso de evaluación de vulnerabilidades de los servidores propuestos. Este proceso se realizará teniendo en cuenta y cumpliendo tres etapas o fases importantes las cuales se describen a continuación:

- **Instalación y parametrización:** para el proceso de se debe contar con un ambiente de pruebas sobre el cual se realice la instalación de cada una de las herramientas, junto con los agentes asociados a tres servidores que cuenten con las mismas características de software.

- **Escaneo de vulnerabilidades:** se realizaría un escaneo con cada una de las herramientas cada uno de los servidores de pruebas propuestos.

- **Análisis de resultados:** en esta parte del proceso se analizan los resultados del escaneo arrojados por cada una de las herramientas, donde en teoría debería mostrar los mismos números de resultados encontrados, en este punto, se debe evaluar la profundidad del escaneo de cada una de las vulnerabilidades halladas, para lo cual se deben de clasificar según su criticidad que estas tenga y si cuenta con un método de solución.

Luego de este proceso, se debe realizar un análisis de costo-beneficio de cada herramienta, donde se deberá tener en cuenta cada una y cuantos equipos soporta la solución, con el fin de determinar los costos de capacitación, tiempos de escaneo y características sobresalientes con respecto a las demás.

2.2 Costo de adquisición:

Inicialmente se debe evaluar el costo de compra de cada una de las herramientas de escaneo. Además, se debe tener en cuenta los costos de configuración y puesta en marcha, así como los costos de entrenamiento para el equipo de seguridad que utilizará estas herramientas.

2.2.1 Costo de mantenimiento:

Consideración de los costos recurrentes, tales como las licencias de software, soporte técnico y actualizaciones de software, esto con el fin de garantizar que las herramientas sigan siendo efectivas en el tiempo que se encuentren operativas.

2.2.3 Tiempo de configuración

Evaluar el tiempo y la complejidad destinado a configurar cada herramienta para la puesta en marcha. Si una herramienta requiere más tiempo para configurarse y usar que otra, esto puede ser un factor importante en la elección.

2.2.4 Precisión de detección

Evaluar la precisión de cada herramienta en cuanto a la detección de vulnerabilidades conocidas y desconocidas en los servidores a intervenir. Se pueden tener en cuenta informes anteriores de pruebas independientes para cotejar los datos y resultados.

2.2.5 Funcionalidad y características

Analizar las características y funcionalidades de cada herramienta, tales como: la capacidad de integrarse con otras herramientas de seguridad, la facilidad de uso, el nivel de personalización de reportes y las opciones de informes generados por host.

2.3 Técnica para la recolección de información

Con el fin de lograr evaluar la efectividad de la metodología planteada, así como la capacidad de poder identificar si esta cumple con los objetivos propuestos, se utilizaría la técnica denominada métodos estadísticos para la recolección de la información.

2.3.1 Métodos estadísticos

Esta propuesta está basada en los datos de pruebas que nos permiten evaluar un porcentaje inicial de equipos de la empresa, la cual está representada en el 20% de los activos de información, principalmente en servidores quienes soportan los aplicativos y servicios críticos para la entidad.

El porcentaje de activos se ve representado en:

- Aplicaciones de Core (plataformas, Bases de datos)
- Activos de información ubicados sobre los ambientes de pruebas, previos y productivos.
- Activos de información clasificados por su criticidad
- Activos de información de redes

2.3.2 Activos evaluados

En la actualidad, Cablefibra Plus cuenta con una serie de servidores Windows los cuales se encuentran divididos en varios ambientes donde se desarrollan en implementan los servicios y aplicativos mediante los cuales la empresa opera y están definidos de la siguiente manera:

ACTIVO	CANTIDAD
Activos Ambiente Desarrollo	20
Activos Ambiente Pruebas	15
Activos Ambiente Producción	13
TOTAL DE ACTIVOS	48

Tabla 2. Activos actuales Cable Fibra Plus

Esta propuesta tiene como foco principal aplicar dicha metodología sobre las vulnerabilidades previamente identificadas sobre los servidores Windows, teniendo en cuenta la criticidad y el impacto que estas tienen sobre los aplicativos y servicios, adicionalmente, esta misma metodología puede ser aplicada a estaciones de trabajo de usuarios.

Teniendo en cuenta que semanalmente se realiza un comité de gestión de cambios, se organizan las áreas en una tabla la cual se relaciona a continuación:

AREA	ALCANCE	NIVEL
Soporte Windows	Servidores Windows	1
Bases de Datos	Bases de datos SQL y Oracle	1
Mesa de Soporte	Estaciones de trabajo	1
Capa Web	Servicios Web	2
Capa Aplicación	Proveedores de Aplicaciones	2
Telecomunicaciones	Infraestructura de red	1

Tabla 3. Áreas Cable Fibra Plus

En esta tabla se encuentran definidas las áreas que conforman el comité de control de cambios, donde cada una de ellas puede verse impactada por la ejecución de una ventana de remediación de vulnerabilidades, lo cual está sujeto a la definición del impacto que estas actividades puedan tener sobre cada una de estas. Con base en la tabla y para el proceso de remediación, se determina que, si la vulnerabilidad previamente identificada y socializada no puede ser remediada por el ingeniero o administrador del servidor, esta debe escalarse a un especialista de seguridad. Adicionalmente, debido a que la infraestructura cuenta con los ambientes de desarrollo, previos y productivos, se debe aclarar que toda aquella actividad que se plantee programar y el tiempo que esta requiera para remediar las vulnerabilidades está sujeta a la criticidad que esta tenga durante el análisis previo con los lideres de área y el cual está clasificado de la siguiente manera:

- Activos productivos y de Core: son los activos críticos de la entidad y fundamentales para la correcta ejecución de los procesos.
- Activos productivos que no son de Core: son los activos de producción para la operación interna de las diferentes áreas.
- Activos no productivos: son los activos que se encuentran en los ambientes de desarrollo y pruebas, los cuales no comprometen la operación ni el Core del negocio.

2.4 Proceso de Remediación

El proceso consiste en realizar las recomendaciones y buenas prácticas para la gestión y aseguramiento de los sistemas operativos con Windows Server, esto para realizar las actividades de remediación de manera adecuada y que los servidores intervenidos no sean afectados después la intervención

2.4.1 Recomendaciones para la correcta remediación de vulnerabilidades

- Por parte del equipo de pruebas funcionales se debe realizar el correspondiente levantamiento de información previo a las actividades de remediación y debe ser socializado con el equipo de remediadores.

- Se deberá solicitar el diligenciamiento de los formatos de checklist correspondientes al servicio intervenido.

- La ejecución de las pruebas funcionales debe ser realizada por el dueño del servicio intervenido para garantizar y/o reportar fallas oportunamente en caso de posibles fallas.

- La ejecución de las actividades de remediación implica cambios sobre la infraestructura por lo que se tener en cuenta una ejecución de pruebas antes, durante y después de cada cambio para verificar el funcionamiento de los servicios intervenidos.

- Se debe generar el correspondiente documento donde se almacene evidencias del procedimiento de remediación y guardarlo en la ruta designada por el área de infraestructura.

- Las actividades de remediación se deben encontrar segmentados por servicio, por lo que es necesario realizar el análisis del escaneo de vulnerabilidades para identificar parámetros como puertos, versión de las aplicaciones y la interacción con otras plataformas esto para identificar posibles fallas posteriores a la actividad de remediación.

2.4.2 Procedimiento General

Estos prerrequisitos fueron planeados y definidos en conjunto con los coordinadores de los servicios y el equipo de infraestructura de Cable Fibra Plus basados en las posibles afectaciones a los servidores intervenidos.

2.4.2.1 Prerrequisitos

Dentro de las actividades previas a la ejecución de las ventanas de mantenimiento sobre los servidores, se debe realizar previamente una validación de prerrequisitos, los cuales son fundamentales para determinar el estado del servidor, capacidades de almacenamiento, validación del sistema operativo, plantillas de hardening aplicadas y accesos a los mismos, con el fin de asegurar que el ingeniero pueda ejecutar la actividad sin ningún inconveniente. Adicionalmente, se establecen los siguientes requisitos para las actividades de remediación de vulnerabilidades:

- Backup o Snapshot del servidor a intervenir
- Informe generado por la herramienta de análisis de vulnerabilidades
- Levantamiento de información del servicio.
- Pruebas funcionales

2.4.2.2 Informe Inicial de Vulnerabilidades

Se debe generar el informe inicial que contenga el resumen de vulnerabilidades encontradas en los servidores a intervenir, esto previo a la actividad.

2.4.2.3 Análisis del informe inicial

Se deberá analizar la información contenida en el informe inicial de análisis de vulnerabilidades para definir cuáles de estas se pueden remediar de acuerdo con las condiciones y restricciones previamente socializadas con los líderes de los servicios.

2.4.2.3 Ejecución de Actividad

Se procederá a ejecutar las actividades de remediación de acuerdo con los documentos generados por el área de investigación, donde se especifica las correspondientes configuraciones del sistema operativo y actualizaciones de seguridad permitidas para el servicio en concreto.

2.4.2.4 Escaneo post actividad

Posterior a la actividad, se deberá realizar la ejecución de un análisis de vulnerabilidades para confirmar que efectivamente se hayan remediado las vulnerabilidades.

2.4.2.5 Pruebas Funcionales

Por último, se debe solicitar la ejecución de pruebas funcionales al dueño del servicio y los resultados de estas.

2.4.3 Posibles afectaciones por ejecución de actividades de remediación

La ejecución de actividades de remediación sobre los servidores Windows realiza cambios importantes sobre el sistema operativo, por lo que es posible que se puedan presentar afectaciones sobre la comunicación, archivos, funcionamiento y transacciones de aplicativos alojados, por lo cual es necesario realizar reinicios sobre los servidores intervenidos y/o motores de base de datos en caso de que aplique.

2.4.4 Beneficios post remediación

Con las actividades de remediación se reduce el riesgo de materialización de explotación de las vulnerabilidades asociadas a Windows Server. Con las actualizaciones de seguridad suministradas por Windows se remedian:

- Vulnerabilidades de Zero-Day.
- Prevención de ataques de malware
- Remedia vulnerabilidades conocidas hasta la fecha

Adicional por medio de configuraciones de políticas locales y de registros se deshabilitan características y puertos que no sean requeridos para la operación de las aplicaciones alojadas en los servidores, lo que disminuye el riesgo a causa de explotación de vulnerabilidades.

3. Resultados

De acuerdo con lo planteado en esta consultoría y con base en las actividades que se recomiendan para ejecutar de manera correcta la implementación de la metodología propuesta para la identificación y remediación de vulnerabilidades, se espera que la empresa genere un proceso robusto de seguridad, que se encuentre apoyado por los altos directivos y que involucre a las diferentes áreas transversales que hacen parte de la operación, las cuales se ven directamente impactadas por estas actividades de remediación, junto con la creación y estructuración de un equipo de seguridad especializado que se encargue de todo el proceso de análisis, identificación, mitigación y validación de resultados, los cuales deben ser presentados en las jornadas de seguridad donde se realice el respectivo seguimiento a estas actividades, sobre las cuales se debe ilustrar cuales son los porcentajes de avance y mitigación de vulnerabilidades de acuerdo con el plan de trabajo definido sobre cada servidor.

Adicionalmente, durante la implementación de la consultoría se espera contar con las memorias del proyecto, donde se documente todo el proceso realizado, las lecciones aprendidas y todo lo relacionado con la metodología aplicada, esto con el fin de poder sustentar la efectividad de la misma, argumentando los beneficios que esto ha traído para la compañía, en aras de mejorar la postura de seguridad frente a los posibles riesgos que se puedan presentar durante un ataque.

4. Discusión

Dado los resultados obtenidos de la solución que se propone se debe considerar los siguientes aspectos para tomar la mejor decisión teniendo en cuenta las necesidades de la empresa Cablefibra Plus y el entorno donde se va a implementar:

Funcionalidad: Debe ser capaz de detectar una amplia gama de vulnerabilidades, como inyecciones de código, cross-site scripting (XSS), vulnerabilidades de configuración, entre otras.

Cobertura de plataforma: La herramienta sea compatible con las plataformas y tecnologías utilizadas en la empresa, ya sea sistemas operativos, aplicaciones web, bases de datos, servidores, etc.

Precisión: La precisión de la herramienta es vital para evitar falsos positivos o negativos. Se debe tener en cuenta la reputación de la herramienta y buscar referencias de otros usuarios para evaluar su nivel de precisión. Se sugieren Foros de Gartner.

Actualizaciones y soporte: la herramienta debe contar con actualizaciones de manera regular para abordar nuevas vulnerabilidades y si hay un equipo de soporte dedicado disponible en caso de problemas o consultas.

Integración con otros sistemas: La herramienta se debe integrar con otros sistemas de seguridad teniendo en cuenta que ya se cuenta con firewalls, sistemas de gestión de incidentes, etc.

Evaluaciones y pruebas: Realizar pruebas de evaluación con versiones de prueba de diferentes herramientas antes de tomar una decisión final.

Informes y análisis: Debe ser capaz de proporcionar información relevante y priorizar las vulnerabilidades de acuerdo con su gravedad.

Costo: Considerar el costo de adquisición y licencia de la herramienta, así como los costos adicionales asociados, como mantenimiento, actualizaciones o soporte técnico.

Facilidad de uso: La herramienta debe ser fácil de usar e intuitiva, tanto para la configuración como para la interpretación de los resultados.

5. Conclusiones y recomendaciones

5.1 Conclusiones

Para concluir, se debe tener presente que los atacantes se han vuelto más audaces en sus intentos de irrumpir de manera ilegal en las redes seguridad y las infraestructuras críticas de las empresas, así como los índices de ciberataques están en su punto más alto, los cuales tendrán éxito si a través de sus ataques de fuerza bruta y demás medios descubren debilidades que puedan ser explotadas en su beneficio. Por eso, todas las empresas independientemente de su tamaño necesitan escaneos de vulnerabilidades ejecutados de forma constante y automática.

Tanto Nexpose, Qualys y Nessus Professional. son excelentes herramientas para escanear la infraestructura informática. Los resultados revelan que el número de vulnerabilidades de seguridad detectadas por las distintas tecnologías varía significativamente, variando el entorno y las configuraciones que estos tengan.

Por último, se debe aclarar que estas herramientas no encontrarán todos los servicios afectados en los sistemas. Los expertos en seguridad por lo general prefieren utilizar Nessus para auditar los sistemas informáticos, sin embargo, esta elección está sujeta a la previa evaluación y beneficios que estas tengan para la organización. Cada opción tiene el potencial de mejorar la postura de seguridad para la organización con el fin de mitigar las vulnerabilidades descubiertas, así como el contribuir a una infraestructura más segura.

5.2 Recomendaciones

Como recomendación y teniendo en cuenta el diseño metodológico previamente propuesto, el cual es la guía fundamental para cumplir con todo el proceso de análisis y remediación de vulnerabilidades, las organizaciones deben entender inicialmente el contexto de la actualidad de su infraestructura y así mismo evaluar cuáles de sus activos de información son los más críticos y sobre los cuales se debe empezar a trabajar, para así dedicar los recursos y esfuerzos en controlar aquellas vulnerabilidades que puedan afectar la operación de manera parcial o total, esto debe estar sustentado en el análisis de impacto de negocio y en los planes de riesgo con los que tenga actualmente la empresa. La efectividad de este plan de trabajo depende en gran parte del compromiso de las directivas y los recursos que destinen para mejorar la postura de seguridad de la organización.

Bibliografía

AboElFotoh, H. M. F., Iyengar, S. S., & Chakrabarty, K. (2005). Computing reliability and message delay for cooperative wireless distributed sensor networks subject to random failures. IEEE Transactions on Reliability, 54(1), 145–155.

Cortés Santamaría, B. (2021). Caso práctico de una prueba de concepto de tres herramientas de gestión y análisis de vulnerabilidades.

Daimi, K., Francia, G., Ertaul, L., Encinas, L. H., & El-Sheikh, E. (2017). Computer and Network Security Essentials. Springer International Publishing. https://books.google.com.co/books?id=b7swDwAAQBAJ

Dalziel, H., & Caceres, A. (2014). How to Attack and Defend Your Website. Elsevier Science. https://books.google.com.co/books?id=VAIbBQAAQBAJ

Deckard, J. (2005). Buffer Overflow Attacks: Detect, Exploit, Prevent. Elsevier Science. https://books.google.com.co/books?id=NYyKhOqOCF8C

Giménez Campos, J. (2020). INTEGRACIÓN Y PROGRAMACIÓN DE SEGURIDAD INTELIGENTE EN REDES IoT.

Göbel, J. G., & Dewald, A. (2011). Client-Honeypots: Exploring Malicious Websites. De Gruyter. https://books.google.com.co/books?id=3BhPZi0C2EUC

Gómez, A. (2014). Enciclopedia de la Seguridad Informática. Madrid. In España.

Karimipour, H., Srikantha, P., Farag, H., & Wei-Kocsis, J. (2020). Security of Cyber-Physical Systems: Vulnerability and Impact. Springer International Publishing. https://books.google.com.co/books?id=yuHyDwAAQBAJ

Kurniawan. (2017). ANALISIS Y GESTION DE VULNERABILIDADES DE SISTEMAS INFORMATICOS CON SOFTWARE LIBRE (AGVISL). 経済志林, 87(1,2).

Marcillo Parrales, M. P., Marcillo Castro, J. C., Ortiz Hernández, M. M., & Mero Lino, E. A. (2020). ANÁLISIS DE LAS HERRAMIENTAS Y TÉCNICAS UTILIZADAS EN PRUEBA DE PENETRACIÓN PARA LA DETECCIÓN DE VULNERABILIDADES EN APLICACIONES WEB. UNESUM-Ciencias. Revista Científica Multidisciplinaria. ISSN 2602-8166, 5(1). https://doi.org/10.47230/unesum-ciencias.v5.n3.2021.316

NEXNET. (n.d.). Función de carga de la pasarela - Soluciones NexNet. Charing Gateway. Retrieved September 24, 2017, from http://nexnetsolutions.com/solutions/telecom-service-providers/oss-bss-solutions/charging-gateway/

Pelton, J., & Singh, I. B. (2015). Digital Defense: A Cybersecurity Primer. Springer International Publishing. https://books.google.com.co/books?id=UIvDCgAAQBAJ

Peñafiel Lucy, K. A. (2021). Factores que determinan la Vulnerabilidad Informática y el Desarrollo de una aplicación móvil para concientizar sobre los Impactos en los Activos. Fides Et Ratio, 21, 1–30. http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2021000100009&lang=es

Sánchez-Sánchez, P. A., García-González, J. R., Triana, A., & Perez-Coronell, L. (2021). Medida del nivel de seguridad informática de las pequeñas y medianas empresas (PYMEs) en Colombia. Información Tecnológica, 32(5), 121–128. https://doi.org/10.4067/s0718-07642021000500121

Van der Linden, M. A. (2019). Testing Code Security. Taylor & Francis Limited. https://books.google.com.co/books?id=C3CbyAEACAAJ

Villora Divino, B. (2018). Evaluación y gestión de vulnerabilidades: Cómo sobrevivir en el mundo de los ciberataques. Universitat Politècnica de València.

Yan, I., Montoya, C., Victor, I., Verdezoto, H., Andrea, I., & Ramírez, V. (2019). Ciberdefensa, Ciberseguridad Y Sus Efectos En La Sociedad. In International Multilingual Journal of Science and Technology (IMJST) (Vol. 4).

Alert, A. (2021). *Alerta para organizaciones colombianas : Cómo enfrentar la dura realidad del estado de ransomware en el país*. 1–6.

Barinas, A., Alarcon, A., & Callejas, M. (2014). Vulnerabilidad de ambientes virtuales de aprendizaje utilizando SQLMap, RIPS, W3AF y Nessus. *Ventana Informática*, *30*, 247-26 0.

Guide, G. S. (2006). Getting Started Getting Started Guide. *Access*, *October*, 1–25.

Id, C. V. E. (n.d.). *Tutorial de qualysguard v6.7 modulo de vulnerability management*.