Análisis de vulnerabilidades y potenciales falencias de la empresa “Servicios TI” frente al Ransomware.

Alex Felipe Escobar Betancur
Arley Yovani Trujillo Villa
Noviembre- 2019

Corporación Universitaria Minuto de Dios - Uniminuto
Tecnología en Gestión de Redes y Comunicaciones
Proyecto de Grado

Resumen

Con el desarrollo de este proyecto de grado sobre el análisis de vulnerabilidades y remediaciones relacionadas al malware encargado del secuestro de información denominado "Ransomware" y los programas informáticos de día cero, los cuales son ataques informáticos creados en una fecha determinada, en la cual no se ha encontrado una corrección por parte de los fabricantes de plataformas de antivirus y antimalware, se pretende encontrar cuales son los principales medios por los cuales podría verse comprometidos los sistemas de información y datos sensibles de la empresa "Servicios TI", así como analizar cuáles serían los impactos que alcancen las amenazas cibernéticas contemporáneas y como se podrían proteger para no ser una víctima de estas.

Palabras Claves: Vulnerabilidad, brecha de seguridad, Malware, Ransomware, Phishing, remediación e información.

Abstract

With the development of this degree project on the analysis of vulnerabilities and remediations related to malware in charge of the information section called “Ransomware” and zero-day software, the computer attacks created on a given date, in which no has found a correction on the part of the manufacturers of antivirus and antimalware platforms, it seeks to find which are the main means by which we could see the information systems and sensitive data of the company “Servicios TI” compromised, as well as detect problems specific impacts that contemporary cyber threats reach and how they could be protected from being a victim of them.

Keywords: Vulnerability, security breach, Malware, Ransomware, Phishing, remediation and information.

Introducción

Un “Troyano informático”, es conocido como un tipo de software malicioso que se presenta al usuario bajo la apariencia de un programa aparentemente legítimo e inofensivo que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado y pudiendo ingresar al equipo de la víctima, el ciberdelincuente puede realizar múltiples acciones, tales como el robo de información, daño a sistemas o servicios, eliminar datos, realizar modificaciones, entre otros.

Los troyanos se concibieron como una herramienta para causar daños en los equipos infectados. Sin embargo, se observa que, en la actualidad, la tendencia ha cambia do hacia el robo de datos bancarios e información personal, ello debido al mayor uso de Internet, en particular, en todo aquel espacio donde se vuelca gran cantidad de este tipo de información sensible.

La ejecución este proyecto de grado, se realiza por una gran pasión con lo relacionado a la seguridad de la información; se puede encontrar posibles mejoras a falencias o vulnerabilidades que pueda presentar “Servicios TI” y que puedan afectar datos sensibles de la compañía o alguno de sus clientes.

Se sabe que la seguridad informática es un campo muy grande, el cual no se podría comprender en su totalidad en la realización de este trabajo, por lo cual se decide su enfoque a investigar las vulnerabilidades que puedan llegar a presentar las amenazas cibernéticas tipo Ransomware o el secuestro de información a los servidores productivos de la compañía y de los equipos de usuarios que estén directamente conectados en la misma red a estos recursos.

Tabla de Contenidos

Lista de figuras

Lista de Tablas

Listado de Anexos

Capítulo 1

Descripción del proyecto

Planteamiento del problema

Cada vez se perciben más casos de Ransomware en todo el mundo, la cual es una estrategia de extorsión digital que permite a los atacantes encriptar los ficheros almacenados en los dispositivos de las víctimas, tales como computadores, celulares, servidores, entre otros y solo los desbloqueen después de recibir dinero a cambio.

Un ejemplo de lo anterior, le sucedió la empresa de telecomunicaciones "Telefónica", en el año (2017), cuando un malware tipo Ransomware, llamado "WannaCry", infectó uno de sus equipos y se propagó por toda su red interna. Tal y como lo expresa la editorial El Tiempo en uno de sus artículos "El gigante de las telecomunicaciones español Telefónica fue víctima el viernes de un incidente de ciberseguridad en su red corporativa que lo obligó a apagar todos los computadores de su sede en Madrid (España) como medida preventiva". (CON AFP Y EFE, 2017).

La empresa PANDA Security, fabricantes de Antivirus y expertos en seguridad, publica algunas cifras alarmantes acerca de las amenazas informáticas, que han surgido en el último tiempo, en el artículo compartido por dicha institución, (Panda Security, 2018) se menciona lo siguiente: "Solo en este año (según los datos que hemos recopilado hasta el 20 de septiembre de 2017), desde PandaLabs hemos registrado 15.107.232 ficheros de malware distintos que no habíamos visto nunca con anterioridad. ¡Más de 15 millones de ficheros totalmente nuevos! Pero el número total de malware que ha sido creado es mucho

mayor: 75 millones, o lo que es lo mismo, 285.000 nuevos ejemplares de malware cada día".

En otro informe publicado por la empresa experta en seguridad "Kaspersky", habla de que Colombia es uno de los países más atacados por ciberdelincuentes en la región y las cifras van en aumento, "Los ataques por Ransomware en América Latina han experimentado un aumento anual de 30% entre 2016 y 2017, con 57.512 detecciones en 2016 y 24.110 hasta la fecha en 2017" (Kaspersky Lab, 2017).

El principal motivo por el cual los ciberdelincuentes realizan este tipo de ataques, es poder sacar un provecho económicamente, puesto que las personas o empresas por el desespero y/o necesidad de obtener la información, están pagando por el rescate de la misma, la cual se exige en un tiempo determinado, por lo general 48 horas. Dicho pago se debe realizar en una criptomoneda denominada "Bitcoin", la cual es una moneda virtual, que utiliza diferentes medios de encriptación para evitar que el beneficiario sea identificado.

Las técnicas utilizadas por los ciberdelincuentes para infectar a un equipo o una red completa con este tipo de malware normalmente son del siguiente modo: la víctima (esta puede ser empleado o un equipo de un invitado), descarga el programa malicioso o da clic en un enlace de un correo "malicioso", e instala algún software responsable del cifrado indebido de los archivos. Luego de cifrar estos, el atacante recibe de la víctima una llave privada (una cadena de texto y caracteres larga) y esta es la única que permite el descifrado de la información comprometida.

Esta problemática pertenece al área de la seguridad informática y desde esta, se pretende investigar y posteriormente proponer unas mejores prácticas o técnicas para mitigar la posibilidad de que Servicios TI, sea víctima de estos programas maliciosos.

Con lo expuesto anteriormente surgen algunas dudas, ¿Está preparado totalmente Servicios TI, contra amenazas de día cero (Tiempo entre cuando se publica una amenaza y se brinda una actualización para progrese en contra de ella), similares al Ransomware o sus variantes?, ¿Cuál es el nivel de madurez de la seguridad de la información en Servicios TI?

Con base a estas inquietudes, se busca realizar un análisis, en el cual se obtengan resultados sobre el estado actual en cuanto a seguridad informática de Servicios TI y así plantear estrategias que ayuden a mitigar en gran medida la pérdida de información por ataques, desconocimientos del usuario o vulnerabilidades de seguridad.

También es necesario indagar si existen trabajos de previos similares al que se realizará y apoyarse en estos, para así lograr diseñar unas estrategias de seguridad informática más robustas, debido a que las amenazas informáticas cada día están creciendo y variando tal y como lo asegura la empresa experta en seguridad informática "SonicWall", (2018), "El año pasado hubo un 71,2% menos de ataques de Ransomware. Sin embargo, el número de variantes aumentó notablemente en un 101,2%.".

Justificación

La importancia de desarrollar este proyecto de grado es conocer los métodos de seguridad informática con los que cuenta actualmente Servicios TI, como protege su información y que tipo de sistemas tiene implementados para prevenir y contrarrestar un eventual ataque de seguridad informática tal como un Ransomware, Phishing, SQL Injection, XSS (Cross Site Scripting) y redes de Botnets. Adicionalmente, se busca implementar estrategias basadas en mejores prácticas, sobre la prevención de este tipo de ataques informáticos.

Los principales beneficiados con este trabajo de investigación y su aplicación serían directamente el personal administrativo de Servicios TI, puesto que ante una afección de malware tipo Ransomware, Botnets, Troyanos, etc. toda su información de sus labores diarias no se vea comprometida. No obstante, también se verían beneficiados indirectamente todos los clientes que tengan información contenida en los servidores de la compañía, debido a que, con la aplicación de estas mejores prácticas, su información contaría con una mejor protección frente a amenazas de seguridad.

Para los estudiantes de Gestión de Redes y Comunicaciones de UNIMINUTO, es de mucho valor la realización de este proyecto, porque para poder determinar el estado de los sistemas de seguridad informática de la empresa, se adquieren conocimientos sobre la actualidad de la seguridad de los datos y como se trabaja en el contexto local.

La ejecución del proyecto es viable, puesto que se le estaría presentando a la empresa Servicios TI un análisis y mejoras a sus procesos de la protección de la información, no acarrearía ningún costo y se podría llegar a prevenir pérdida de información invaluable para la empresa y sus clientes.

Los riesgos de no llevarse a cabo este proyecto de grado en la empresa Servicios TI, es que posiblemente al no analizar los procedimientos de prevención ante estos ataques de malware, se estaría facilitando a los atacantes, hacer uso de la información empresarial y de sus clientes y en caso de presentarse un robo de información o una afectación de la integridad de la misma, perdería credibilidad con los clientes y su reputación se vería seriamente afectada.

Objetivo general

Implantar estrategias de seguridad de la información, con el fin de reducir posibles vulnerabilidades relacionadas al secuestro de información (Ransomware), que sea crítica para la continuidad de la operación de la empresa “Servicios TI”.

Objetivos específicos

1. Realizar un análisis de madurez en cuanto a seguridad de la información para así determinar en qué estado se encuentra la empresa y las posibles mejoras a implementar.

2. Identificar las principales vulnerabilidades relacionadas al secuestro de información (Ransomware), riesgo de pérdida de información y niveles de conocimiento de las personas que de manera directa o indirecta tienen acceso a los sistemas de información de la empresa.

3. Ejecutar correcciones y planes de mejora continua a los equipos, sistemas de información o aplicativos a los cuales se les haya encontrado vulnerabilidades criticas relacionadas al secuestro de información por Ransomware.

Metodología a Utilizar

La ejecución del proyecto se realizará por medio de fases, las cuales son tres (3) y se describen con sus respectivas actividades a continuación:

FASE 1: Análisis de Madurez

Actividad 1: Realizar una encuesta a los administradores de cada plataforma, sobre configuraciones, mejores prácticas, publicaciones, actualizaciones, documentación y planes de contingencia de los principales recursos necesarios para la continuidad de la operación.

Actividad 2: Realizar una calificación, según estándares y buenas prácticas a cada uno de los ítems (Servidores, publicaciones, servicios expuestos, versión de servidores, gestión de accesos, gestión de proveedores, etc.).

Actividad 3: Finalizar la ponderación de cada uno de los recursos para así obtener un indicador a nivel “Macro”, del nivel de madurez de toda la plataforma tecnológica.

Tratamiento de la información de la Fase 1

La información en esta fase, será obtenida a partir del conocimiento de cada analista responsable de cada plataforma (Gestión de redes, Servidores, cloud, Virtualización, CCTV, etc.).

Tiempo estimado para su ejecución: 2 meses.

FASE 2: Análisis de vulnerabilidades enfocado en Ransomware

Actividad 1: Realizar análisis Pentesting tipo "caja blanca", el cual consta de realizar "Ataques", pruebas o escanear vulnerabilidades, a determinados recursos, con el consentimiento de la compañía, con el fin de encontrar posibles accesos o falencias que pueda ser utilizadas por un Software malicioso tipo "Ransomware".

Para este análisis, se utilizará principalmente la herramienta "Nessus" de la empresa "Tenable", en su versión gratuita. Este análisis se realizará sobre sus recursos inventariados previamente.

Actividad 2: Se realizarán otros análisis de vulnerabilidades con las herramientas gratuitas "OpenVAS y MetaSploit" con el fin de encontrar posibles falencias que el software de la actividad anterior no haya logrado identificar.

Actividad 3: Se realizará un informe ejecutivo evidenciando cuales fueron las principales amenazas encontradas, las cuales puedan ser potencialmente "Explotadas" y puedan causar afectación de servicios.

Actividad 4: Se realizará un análisis de varias estaciones de trabajo, que se encuentren conectadas a la red local, con el fin de encontrar protocolos de comunicación vulnerables a un ataque e infección por Ransomware o alguna de sus variantes.

Actividad 5: Se realizarán un informe ejecutivo, donde a cada una de las vulnerabilidades encontradas, se explicará cómo es la forma en que los "atacantes" o malware, podrían afectar a la organización, así de cuáles son las estrategias para remediar dichas fallas encontradas tanto en servidores, así como en equipos clientes, aplicaciones y demás recursos.

Tratamiento de la información de la Fase 2

Se buscará en Internet documentación sobre las presuntas vulnerabilidades encontradas, con el fin de encontrar soluciones a las mismas. Adicionalmente, se buscarán mejores prácticas recomendadas por fabricantes y expertos en seguridad reconocidos.

Se hará uso de los recursos de Internet.

Tiempo estimado para su ejecución: 3 meses.

FASE 3: Remediación

Actividad 1: Con base en la información recolectada en las actividades anteriores y en conjunto con el personal encargado de cada plataforma de la compañía, se corregirán falencias de seguridad como por ejemplo actualizaciones, configuraciones de plataforma Anti- Spam del correo electrónico, configuraciones y actualizaciones de equipos clientes, ajustes por defecto, publicaciones con información vulnerable expuesta, gestión de accesos de usuarios, desinstalación de software riesgoso, entre otras.

Actividad 2: Auditar que las vulnerabilidades se hayan remediado efectivamente. Esto se puede lograr, realizando análisis de vulnerabilidades a los recursos puntuales donde se encontraron falencias o intentando realizar pruebas de intrusión con una amenaza cuyo funcionamiento y proceso de infección sea similar a un Ransomware.

Tratamiento de la información de la Fase 3

La información en esta fase, será obtenida a partir del conocimiento de cada analista responsable de cada plataforma (Gestión de redes, Servidores, Cloud, Virtualización, CCTV, etc.)

También se obtendrá información de diferentes fuentes confiables de Internet, tales como paginas oficiales de fabricantes, informes de seguridad de expertos en Seguridad, libros y

artículos electrónicos y físicos, que puedan ayudar a remediar las vulnerabilidades encontradas.

Tiempo estimado para su ejecución: 2 meses.

Impactos (de carácter social, económico y aportes al conocimiento)

- A nivel personal, afianzar conocimientos relacionados a la seguridad de la información.
- Aportar a la empresa a mitigar o reducir considerablemente riesgos que puedan poner en peligro información crítica para el negocio.
- Lograr que los usuarios de la compañía tomen conciencia de las acciones que realizan cada que se sienten frente a una pantalla y que estén enterados de los peligros que hay en la actualidad y estrategias para evitarlos.

Capítulo 2

Marco Teórico

En términos de seguridad de la información, se puede definir una vulnerabilidad como una debilidad o falencia que se tiene en un activo (Hardware, Software, aplicación, Acceso a un Sistema), la cual pueda ser aprovechada o "Explotada", por un atacante o una aplicación amenaza informática, lo cual se puede convertir en un potencial riesgo de seguridad. Por lo cual, es necesario realizar un inventario de activos, para realizar una valoración, identificación y priorización de vulnerabilidades críticas, que puedan ser identificadas en un sistema.

Actualmente, existen diferentes normas a nivel internacional, las cuales apuntan a un mismo objetivo: Proteger la confidencialidad, integridad y disponibilidad de la información de un usuario o una organización, así como la de castigar a las personas, empresas que se dediquen al acceso no autorizado, robo, comercialización o sabotaje con información personal o de gran valor para una compañía.

Desde el punto de vista legal en Colombia y según el decreto de ley "1273", de 2009, decretado por el congreso colombiano y el cual se ha denominado "Ley de la Protección de la información y de los datos", estos son los artículos en los que un posible atacante, podría incurrir al intentar acceder a una red, aplicación o sistema de manera no autorizada:

ARTÍCULO 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta

y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269E: USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

ARTÍCULO 2691: HURTO POR MEDIOS INFORMÁTICOS y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Adicional a las diferentes normas que existan a nivel internacional o nacional, es necesario siempre estar en búsqueda de posibles "huecos de seguridad", que puedan ser explotados y puedan causar afectación en una compañía, por lo cual, es recomendable realizar periódicamente un análisis de vulnerabilidades, para lograr identificar posibles debilidades de un sistema informático. Según (Welivesecurity By ESET), los pasos para la realización de dichos análisis son los siguientes:

Obtener la aprobación para la evaluación de vulnerabilidades

Debido a que las actividades relacionadas con la identificación de vulnerabilidades pueden catalogarse como intrusivas por las herramientas de seguridad que se encuentren instaladas dentro la infraestructura de la organización, es necesario que se tenga la aprobación para ejecutar el escáner, programar la actividad y notificar a las partes interesadas, es decir aquellas que pueden afectar o verse afectadas por esta actividad.

Generar un inventario de activos

Una buena práctica relacionada con la gestión de la seguridad consiste en la creación y mantenimiento de un inventario de activos asociados con la información y sistemas, utilizados para procesar, almacenar o transmitir esa información. Una vez que se cuenta con la lista, se deben seleccionar los activos sobre los cuales se llevará a cabo la evaluación. En general, las pruebas se deben enfocar en los elementos críticos, relacionados con los procesos más importantes.

Definir el alcance de la evaluación

Derivado de la generación del inventario y la selección de los objetivos, la evaluación puede ejecutarse de dos modos: interno y externo. Desde la perspectiva interna se realiza el escaneo desde la infraestructura de la organización, con acceso a los recursos de forma directa. La evaluación externa implica lidiar con la protección perimetral que se tiene en la red corporativa y se adopta la posición que tendría un atacante en busca de alguna vulnerabilidad.

Recabar información, identificar y evaluar vulnerabilidades

La evaluación puede realizarse de forma manual o automatizada a través de alguna herramienta, para obtener información relevante en cuanto a las vulnerabilidades en los sistemas considerados. Posterior a la identificación de las debilidades y la obtención de información relacionada con las mismas, resulta necesario llevar a cabo un proceso de valoración que permita conocer su impacto. Para ello es posible utilizar algún sistema de puntaje como CVSS. Es importante mencionar que herramientas especializadas permiten automatizar estas actividades.

Generar un informe de resultados

Con base en los resultados de la evaluación se debe generar un informe que permita conocer el estado de la seguridad en los sistemas a partir de los hallazgos. También busca mostrar los resultados a través de la priorización de las vulnerabilidades, con el objetivo de atender primero las debilidades de mayor impacto sobre los activos.

Generar un plan de remediación

Como última actividad asociada a la evaluación de vulnerabilidades es necesario desarrollar y ejecutar un plan de remediación que permita corregir las fallas identificadas y evaluadas, en conformidad con los resultados de la priorización. En general, la corrección de estas fallas se relaciona con la aplicación de actualizaciones o parches de seguridad" (2014).

Finalmente, aparte de una buena gestión de vulnerabilidades dentro de una compañía, es necesaria la adopción de normas y estándares para así mitigar aún más las brechas de seguridad que se puedan presentar al interior de la compañía. Dichas estrategias, según la experta en seguridad (Aristizabal, 2019), estas son algunas de las estrategias a implementar:

Concientización y capacitación del factor humano, Gestión de vulnerabilidades, Monitoreo y Detección, Aseguramiento de dispositivos móviles, Gestión de contraseñas, Controles USBs, Cifrado, Copias de seguridad, Utilización controlada de Shadow IT y Gestión de Riesgos de ataques internos.

Fases de Ataque del Ransomware

Por lo general el Ransomware tiene 5 etapas de ataque y según explica la empresa experta en seguridad informática "Manage Engine", en un informe publicado en el año 2017, son las siguientes:

1. El usuario descarga un archivo con software malicioso desde un correo, red social, página falsa, entre otros.

2. Una vez descargado, el software se instalará automáticamente e intentará infectar el sistema operativo.

3. El Ransomware intentará escanear otras redes e infectar otros equipos que tengan vulnerabilidades.

4. Posteriormente, infectará todos los archivos del usuario, los encriptará con una llave de "AES-256", el cual es método de cifrado que divide el archivo en pequeños fragmentos y a a cada uno de estos, le aplica una "contraseña" de 256 caracteres de longitud, prácticamente imposible de descifrar.

5. Finalmente, el Ransomware creará una llave única encriptada, la enviará al ciberdelincuente y este pedirá un rescate por la liberación de la información de la víctima.

Adicional a las diferentes normas que existan a nivel internacional o nacional, es necesario siempre estar en búsqueda de posibles "huecos de seguridad", que puedan ser explotados y puedan causar afectación en una compañía, por lo cual, es recomendable realizar periódicamente un análisis de vulnerabilidades, para lograr identificar posibles debilidades de un sistema informático.

Capítulo 3

Desarrollo de la propuesta

Cronograma

A continuación, se presenta el cronograma de trabajo con el tiempo estimado de cada una de las actividades, las cuales fueron distribuidas en 3 fases. El proyecto inició desde el mes de marzo y finalizó en el mes de noviembre.

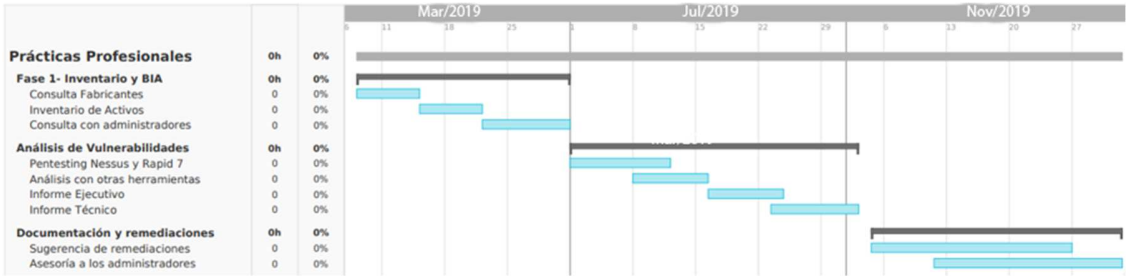


Gráfico 1 Cronograma de actividades

Responsables

Los responsables de llevar a cabo el proyecto de prácticas son los Sres. Alex Felipe Escobar Betancur y Arley Yovani Trujillo Villa, estudiantes de sexto semestre de Gestión de redes y comunicaciones, de la corporación universitaria Minuto de Dios "UNIMINUTO".

Presupuesto

RUBROS	Presupuesto		TOTAL
	Efectivo (en pesos)	**Especie**	
1. Personal	2.500.000	0	2.500.000
2. Equipos	0	3.200.000	3.200.000
3. Materiales e insumos	100.000	0	100.000
4. Transporte local	200.000	0	200.000
5. Servicios Técnicos	0	500.000	500.000
6. Capacitación	800.000	0	800.000
7. Producción intelectual: corrección de estilo, pares evaluadores, traducción, diseño y diagramación, ISBN, impresión u otro formato	100.000	0	100.000
Costo del proyecto	3.700.000	3.700.000	**7.400.000**

Tabla 1. Presupuesto

Las fuentes de ingreso para la financiación y la ejecución del proyecto, fue por cuenta de los estudiantes Alex Felipe Escobar Betancur y Arley Yovani Trujillo Villa.

Capítulo 4

Resultados

El análisis de vulnerabilidades fue desarrollado en la empresa Servicios TI, donde se trabajó con los objetivos y políticas definidas por la misma.

El resultado de este análisis de vulnerabilidades y remediaciones a las brechas de seguridad encontradas, se compartirán en este documento. No obstante, al departamento de TI de la empresa, se entregarán más detalles sobre las vulnerabilidades encontradas en el análisis, con el fin de mantener la confidencialidad y proteger datos sensibles de la compañía.

Inventario de activos, servicios y plataformas tecnológicas: Con este análisis, se busca realizar un inventario de cada uno de los servidores, servicios, plataformas o activos tecnológicos de la compañía. Con el inventario, se busca también dar una ponderación en cuanto a la importancia que significa cada uno de estos recursos para la continuidad del negocio.

El análisis que se presenta a continuación está basado en el modelo de inventario de recursos, desarrollado por la ISO 27001, con el cual se busca tener claro por parte de la empresa, de que activos, plataformas y servicios tiene, de cuál es la importancia de estos para el negocio y de las vulnerabilidades de seguridad que puedan presentar estos.

A continuación, se presenta el resultado del inventario de activos, servicios y plataformas con las cuales cuenta la empresa Servicios TI. Vale la pena resaltar, que, en el presente informe, no se presentarán las verdaderas direcciones IP, usuarios, contraseñas y/o acceso a ninguno de los recursos de la compañía, por temas de confidencialidad e integridad de la información.

La valoración del riesgo que se le ha otorgado a cada recurso es la siguiente:

Gráfico 2. Valoración del riesgo

Y los elementos que se han definido para dar una ponderación a nivel general sobre la clasificación del riesgo que tiene cada uno de los recursos, fueron los siguientes:

Impacto: Es el nivel de afectación que tendía la compañía tanto para el personal externo, como para clientes y proveedores, en caso de que este recurso tuviese una afectación de los servicios que suministra, por un ataque informático.

Esta calificación, se realiza en conjunto con administradores de los diferentes servicios y plataformas de la compañía, puesto que conocen el alcance que tienen cada uno de estos recursos.

Probabilidad: Es la probabilidad de que el recurso sufra un ataque informático. Para este elemento de medición, se tiene en cuenta, si el recurso está expuesto en Internet, si cuenta con una protección Anti-Malware, si cuenta con actualizaciones de su sistema operativo o de su firmware, si está directa o indirectamente conectado a redes de comunicaciones que puedan presentar una amenaza para el mismo.

Clasificación del riesgo en general: El criterio que se tiene en cuenta, para dar la ponderación del riesgo a nivel general del recurso es la siguiente:

ELEMENTOS DE RIESGO				EN GENERAL
IMPACTO		PROBABILIDAD		CLASIFICACIÓN DEL RIESGO
ALTO	+	ALTO	=	ALTO
ALTO		MEDIO		ALTO
ALTO		BAJO		MEDIO
MEDIO		ALTO		ALTO
MEDIO		MEDIO		MEDIO
MEDIO		BAJO		MEDIO
BAJO		ALTO		MEDIO
BAJO		MEDIO		MEDIO
BAJO		BAJO		BAJO

Gráfico 3. Ponderación del riesgo

Inventario de Servidores

		ELEMENTOS DE RIESGO		EN GENERAL
REF	RIESGO DE PROCESO PARA EL NEGOCIO	IMPACTO	PROBABILIDAD	CLASIFICACIÓN DEL RIESGO
S	SERVIDORES			
S1	Lenovo ThinkServer RD640 (x2)	A	M	A
S2	Servidor CLEARPASS	M	B	M
S3	Servidor HERA	A	M	A
S4	Servidor VEEAM-NEWS	M	B	M
S5	Servidor CERBERUS	A	M	A
S6	Servidor AIRWAVE	M	M	M
S7	Servidor VCENTER	M	B	M
S8	Servidor AFRODITA	A	M	A
S9	Servidor ARES	A	M	A
S10	Servidor CAOS	A	M	A
S11	Servidor HADES	A	M	A
S12	Servidor HIEDRA	A	M	A
S13	Servidor ATENEA	A	M	A
S14	Servidor HERMES	A	M	A
S15	Servidor HESFESTOS	A	A	A
S16	Servidor URANO	A	M	A
S17	Servidor PRUEBAS_CLIENTES	B	M	M
S18	Servidor CAMARAS_HESTIA	M	M	M
S19	Servidor ISIS	M	M	M
S20	Servidor PICCOLO_ZABBIX	A	B	M
S21	Servidor PERSEO	M	M	M
S22	Servidor TEAMPASS	A	B	M
S23	Servidor JUPITER_HELPDESK	A	A	A
S24	Servidor DEMETER_ZABBIX	A	B	M
S25	Servidor HOST ESXI 1	A	B	M
S26	Servidor HOST ESXI 2	A	B	M
S27	Servidor ZEUS	A	M	A

Gráfico 4. Inventario de servidores y servicios

En la evaluación del riesgo para los servidores, se realizó inventario de servidores físicos (S1) y los virtuales (S2- S27). Para evaluar la probabilidad de una afectación el primer tipo de servidores se tuvo en cuenta la versión del sistema operativo que tiene instalado y si tenía una conexión directa a la red de datos, mientras que, para los servidores virtuales, se determinaron se tuvieron en cuenta a parte de la versión del sistema operativo, el tipo de aplicativos y versiones que tienen configurados actualmente.

Inventario de servicios y plataformas de redes de datos

SR	SERVICIOS DE RED			
SR1	Switche Core HP A 5120- JG236A (x2)	A	B	M
SR2	Switche LAN HP V1910 - JE007A 24 Ports (X2)	A	B	M
SR3	Switche LAN HP V1910- JG54A 48 Ports	A	B	M
SR4	Canal de Internet UNE (10 Mbps)	A	M	A
SR5	Canal de Internet Claro Banda Ancha (100 Mbps)	A	M	A
SR6	Canal MPLS para clientes 10 Mbps	B	M	A

Gráfico 5 Servicios de Red

En la evaluación del riesgo e inventario de los servicios de redes de datos, se tuvo en cuenta en el impacto, los servicios que podría afectar en caso de una falla en sus servicios. En cuanto a los canales de Internet, tienen una calificación de riesgo Media, debido a que cuentan con direcciones IP públicas que tienen servicios expuestos en Internet, lo cual hace más vulnerables a estos servicios.

Inventario de equipos de seguridad informática

SI	SEGURIDAD INFORMÁTICA			
SI1	UTM Fortigate 60C	A	A	A
SI2	UTM Fortigate 90D	A	A	A
SI2	Consola de Antivirus	B	B	B
SI3	Plataforma AntiSpam	M	M	M

Gráfico 6 Plataformas de Seguridad

En la evaluación del riesgo de los equipos que brindan servicios de seguridad informática y seguridad del perímetro (Dispositivos de red ubicados dentro de la compañía).

La ponderación general, obtuvo un nivel alto para los dispositivos UTM Fortigate, debido a que ambos son sumamente críticos para la operación de la compañía y el análisis de riesgo también es alto, debido a que estos equipos, tienen servicios expuestos en Internet, tales como su pantalla de ingreso y servicios publicados por diferentes canales de Internet.

Inventario de equipos de almacenamiento

A	ALMACENAMIENTO			
A1	SAN HP 3PAR StoreServ 7200	A	B	M
A2	NAS Seagate USM	M	A	A
A3	HP MSA 2040	A	B	M
A4	HP StoreOnce 3540	A	B	M

Gráfico 7 Dispositivos de almacenamiento

El análisis del inventario de dispositivos de almacenamiento, arroja que, el único dispositivo que tiene un riesgo alto de seguridad es la NAS Seagate USM, debido a que tiene un sistema operativo (Firmware) con vulnerabilidades conocidas y que pueden ser explotadas (Aprovechadas).

Inventario de equipos de plataformas de servicios internos

PS	PLATAFORMAS DE SERVICIOS			
PS1	Mesa de Ayuda (GLPI)	A	A	A
PS2	Plataforma de gestión de Accesos (Team Pass)	A	M	A
PS3	Plataforma de gestión documental (DocuSign)	A	M	A
PS4	Software de Gestión Comercial	A	M	A
PS5	Sistema de almacenamiento de archivos- Nube privada (Own Cloud)	A	A	A
PS6	Correo Exchange On-Premise	A	M	A

Gráfico 8 Plataformas de servicios

Con respecto a las plataformas de servicios internos, todas han resultado con una ponderación a nivel general “Alta”, debido a que todas son críticas para las operaciones del negocio y dos de estas, tienen versiones de software, las cuales tienen vulnerabilidades conocidas y que pueden ser explotadas por personas con conocimientos intermedios en seguridad informática.

Inventario de equipos de redes inalámbricas

RI	REDES INALÁMBRICAS			
RI1	Access Point's Aruba Networks	B	M	M
RI2	Plataforma de gestión centralizada Aruba Networks	B	M	M
RI3	Sistemas de control de domótica	B	B	B
RI4	IP CAM- Ubiquiti (CCTV)	B	M	M

Gráfico 9 Redes inalámbricas

Los dispositivos de red inalámbrica, presentan una ponderación a nivel general “Medio”, debido a que estas no tienen publicaciones de sitios y tienen algoritmos de autenticación seguros tales como WPA2- PSK y tipo Radius.

Inventario de equipos de usuario final

EUF	EQUIPOS DE USUARIO FINAL			
EUF1	Equipos portátiles de colaboradores	B	A	M
EUF2	Celulares corporativos de colaboradores	B	A	M
EUF3	Telefonía IP Cisco IP Phone 303	B	M	M

Gráfico 10 Equipos de usuario final

Finalmente, en la calificación de riesgo y de impacto para el negocio, están los equipos de usuario final, los cuales tienen un impacto bajo para la productividad de la empresa, pero dos de estos (Equipos portátiles de colaboradores y Celulares corporativos

de Colaboradores) tienen un riesgo de ser afectados por malware y pérdida de información, debido a que se conectan a redes externas a las de la oficina de Servicios TI y a estos se les conectan dispositivos de los cuales no se pueden comprobar su seguridad.

Análisis de madurez de la seguridad informática

La implementación de un modelo de madurez relacionado con la seguridad de la información de una compañía es un instrumento para ayudar a una organización a evaluar y determinar el grado de avance en la implementación de procesos que conlleven a mejorar la seguridad, confidencialidad e integridad de sus datos.

Para realizar este análisis, se tuvo en cuenta un modelo el cual tiene a disposición, la ISO con su norma 27001, relacionada con la seguridad de la información y como resultado de este, la empresa obtendrá diferentes aspectos de sus procesos de implementación en los cuales quedará claro cuáles son sus fortalezas, sus debilidades, dónde se necesitan mejoras y recomendaciones para mejorar.

En análisis de madurez que se realizó a la empresa Servicios TI, se tuvieron en cuenta 5 aspectos referentes a la seguridad de la información, los cuales están directamente relacionados con las brechas que se puedan presentar para que una herramienta tipo Ransomware, entre en la red de la compañía y pueda causar algún tipo de afectación. Estos aspectos son los siguientes:

- **Visibilidad**: En este aspecto se evaluó si la compañía tiene implementadas plataformas para la visualización en tiempo real de amenazas, las cuales ayuden a tomar decisiones de una manera más acertada.

- Estandarización: Se evaluó si la empresa cumple con estándares relacionados con la organización de sus datos, documentación y bases de conocimiento definidos por organizaciones tales como ITIL, COBIT, AGILE, SCRUM, entre otras.

- Optimización relacionada al UTM: Se analizó los niveles de seguridad que se tienen configurados en la plataforma de seguridad perimetral de la compañía, la cual es de vital importancia, puesto que los servicios críticos para Servicios TI, dependen de este dispositivo el cual unifica y gestiona todas las conexiones entrantes y salientes a Internet.

- Gestión del Riesgo: Se analizó si se realizan análisis de vulnerabilidades y su frecuencia. Además, también se evaluó si se cuentan con plataformas para detener y prevenir ataques especializados tales como Firewall de aplicaciones WEB o un dispositivo con funciones de proteger ataques de denegación de servicios.

- Gestión de Redes WAN y LAN: Se analizó si se tienen configuradas funciones avanzadas de protección de redes cableadas e inalámbricas de la compañía.

- Aseguramiento y afinamiento de redes: En este ítem se evaluó si en la empresa se tiene la gestión de accesos, credenciales y contraseñas de una manera unificada, la cual permita tomar decisiones y actuar de manera eficaz, rápida y eficiente, ante un evento de seguridad de la información.

Cada una de estas categorías, tiene un peso, el cual fue otorgado por el personal de Informática de la compañía Servicios TI. Vale la pena resaltar, que este valor puede variar para cada tipo de modelo de negocio, por lo cual para una empresa el tema del aseguramiento de redes sea irrelevante, para otra empresa esto sea de vital de importancia, para mantener a salvo información importante de la propia empresa y de sus clientes.

Peso General	Categoría
16%	Visibilidad
13%	Estandarización
13%	Optimización (UTM)
25%	Gestión del riesgo
20%	Gestión de red LAN y WLAN
13%	Aseguramiento de Redes

Gráfico 11 categorías de análisis de madurez

El criterio, es el nombre de cata ítem a evaluar, el peso es la importancia que este ítem tiene dentro de la categoría. Por ejemplo, si la categoría "visibilidad", tiene 4 criterios, la suma de estos criterios debe ser el 100%.

El porcentaje de avance es el valor que se da, posterior al análisis de cada uno de los procesos que tiene implementados en la compañía. La ponderación, se saca, multiplicando el porcentaje de avance, por el peso del ítem que se está evaluando.

Visibilidad:

Peso General	Categoria	Criterio	Peso	Avance	Ponderación	Observaciones	Recomendaciones
16%	Visibilidad	Eventos en tiempo real	25,0%	70,0%	17,5%	Visibilidad perimetral y de equipos conectados directa o indirectamente a	Integrar eventos de Firewall, aplicativos comerciales, Bases de Datos y AD a sistems SOC
	Visibilidad	Analisis de aplicativos, servicios y protocolos de red	25,0%	50,0%	12,5%	Herramienta de alertas tempranas y monitoreo	Configuracion de reportes Syslog, Analisis con un Sniffer
	Visibilidad	Monitoreo NOC o SOC (Nagios, Cacti, Zabbix)	25,0%	90,0%	22,5%	Se tiene configurada la herramienta Zabbix	Integrar todos los equipos físicos, tales como NAS, Switches y cámaras a Zabbix
	Visibilidad	Sistemas de Generación de Reportes	25,0%	20,0%	5,0%	Fortianalyzer y Syslog - Reportes completos FAZ	Implementar un dispositivo para realizar reportes, de ser posible, integrar con Zabbix

Gráfico 12 Ponderación de la visibilidad en la red

Estandarización:

Peso Gene	Categoria	Criterio	Pes	Avan	Ponderaci	Observaciones	Recomendaciones
13%	Estandarización	ITIL, COBIT, Agile, Scrum - Gestión de Eventos	20,0%	20,0%	4,0%	No se tiene estructurado con base a un estándar la gestión de eventos y/o derroteros a seguir durante determinada situación de contingencia, instalación o modificación	Adoptar un esquema de documentación tal como lo sugiere ITIL
	Estandarización	ITIL, COBIT, Agile, Scrum - Gestión de Disponibilidad	8,0%	20,0%	1,6%	No se tiene documentación referente a Plan de Recuperación ante desastres	Tener clara la documentación sobre G. disponibilidad (Analisis SPOF o puntos únicos de fallos)
	Estandarización	ITIL, COBIT, Agile, Scrum - Gestión de Incidentes y Re	20,0%	90,0%	18,0%	Se tiene implementada Mesa de Ayuda	Se debe estandarizar la comunicaciones que se den por este medio además de generar reportes y estadísticas sobre el uso de esta plataforma. Se debe implementar Gestión de Problemas.
	Estandarización	ITIL, COBIT, Agile, Scrum - Gestión de Capacidad	13,0%	15,0%	2,0%	No se tiene implementado un Capacity Planning	G Capacidad (Pronosticos), alertas automáticas por consumo de canales y recursos FW (consola y faz)
	Estandarización	ITIL, COBIT, Agile, Scrum - Gestión de Continuidad	13,0%	65,0%	8,5%	Se tienen configuradas réplicas de servidores hacia sitios alternos	Se recomienda tener documentación sobre los procedimientos a realizar en caso de contingencia, también documentación sobre cuando se declara una contingencia y una finalización de esta.
	Estandarización	ITIL, COBIT, Agile, Scrum - Gestión de Configuración	13,0%	20,0%	2,6%	No se tiene un sistema automatizado para configurar equipos o plantillas para servidores y máquinas virtuales	Plan de aprovisionamiento de nuevos equipos, backups automáticos de clientes. Se recomienda un servidor WDS.
	Estandarización	Modelo de operación	13,0%	40,0%	5,2%	Backups Manuales, Hardening sobre Firewall ppal aplicado	Automatizar rutinas, depuración, hardening, documentación

Gráfico 12 Ponderación de la estandarización

Optimización (UTM)

Peso Gene	Categoria	Criterio	Pes	Avan	Ponderaci	Observaciones	Recomendaciones
13%	Optimización (UTM)	Web Filter	20,0%	98,0%	19,6%	Perfiles aplicados a políticas de navegación	Afinar permisos entre usuarios
	Optimización (UTM)	AppControl	20,0%	98,0%	19,6%	Aplicación de APPControl a Wifi y LAN	Trevisar constantemente que aplicativos pueden ser bloqueados por alto consumo de tráfico.
	Optimización (UTM)	IPS/IDS	20,0%	95,0%	19,0%	Gestión de perfiles IPS	Revisar si es necesario eliminar firmas o agregar nuevas firmas sobre perfiles de IPS de sitios WEB
	Optimización (UTM)	DoS	20,0%	90,0%	18,0%	Gestión de perfiles DoS	No es equipo dedicado (Capacidad del Fortigate), se debería contar con un equipo especializado
	Optimización (UTM)	QoS	20,0%	40,0%	8,0%	Se tienen reglas de QoS muy básicas	Aplicar QoS para canales de internet

Gráfico 13 Ponderación de la Optimización de UTM

Aseguramiento de Redes

Peso Gene	Categoria	Criterio	Pes	Avan	Ponderaci	Observaciones	Recomendaciones
13%	Aseguramiento de Re	Autenticación VPNs	20,0%	98,0%	19,6%	Existen algunos usuarios locales en la plataforr	Eliminar usuarios locales de VPN SSL y trabajar todos por LDAP
	Aseguramiento de Re	Autenticación Multifa	18,0%	0,0%	0,0%	No existe plataforma de autenticación multifa	Implementar en UTM y sistema comercial
	Aseguramiento de Re	Servicios de Identidad de Red y	17,0%	20,0%	3,4%	Security en Switches, ni acceso a nevegación por usuario de directorio activo.	Integrar UTM al AD, para permitir la navegación por perfiles de navegación. Implementar Port Security en Switches que lo permitan.
	Aseguramiento de Re	Autenticación de Con	19,0%	80,0%	15,2%	Autenticación de WLAN con NPS, FSSO para na	Falta tener más control en equipos que se conectan a redes de invitados.
	Aseguramiento de Re	Certificado Digital	26,0%	0,0%	0,0%	No se tienen certificados SSL emitidos por una	Adquirir certificados SLS para el sitio principal, MDS y servicios publicados.

Gráfico 14 Ponderación del aseguramiento de redes

Gestión de red LAN y WLAN

Peso Gene	Categoria	Criterio	Pes	Avan	Ponderaci	Observaciones	Recomendaciones
20%	Gestion de red LAN y	Control de VLANs y Su	18,0%	98,0%	17,6%	Falta documentación del subnetting	Centralizar inventario de VLANs, definir consecutivos de direccionamiento, sumarizar vlans actuales.
	Gestion de red LAN y	Inventario de activos	18,0%	50,0%	9,0%	Se tiene marcación de puntos de red, falta doc	Definir inventario de equipos y puertos de forma centralizada
	Gestion de red LAN y	Gestión de direcciona	12,0%	80,0%	9,6%	Se tiene control de las publicaciones, pero falt	Documentación de publicaciones
	Gestion de red LAN y	DMZ y zonas seguras (	13,0%	40,0%	5,2%	Definir Subredes DMZ para publicación de serv	Politicas entre DMZ y LAN, políticas entre VLAN
	Gestion de red LAN y	Estado de salud en re	15,0%	25,0%	3,8%	configuraciones y hardening de networking de la compañía	Optimización de Spanning Tree y protocolos L2, Site Survey
	Gestion de red LAN y	Adecuaciones Fisicas	12,0%	98,0%	11,8%	Falta documentación sobre el cableado del Da	Crear documentación centralizada sobre las conexiones del Datacenter
	Gestion de red LAN y	Control de acceso y perfiles de usuarios	12,0%	50,0%	6,0%	Cambiar contraseñas y accesos periodicamente de Switches y Firewall	Afinamiento de perfiles para administración de equipos.

Gráfico 15 Ponderación de la Gestión de red LAN y WAN

Resultados del Análisis de Madurez

El resultado del análisis, arrojó que le empresa "Servicios TI", actualmente, está en un 59.1 % de implementación de sistemas de seguridad de la información.

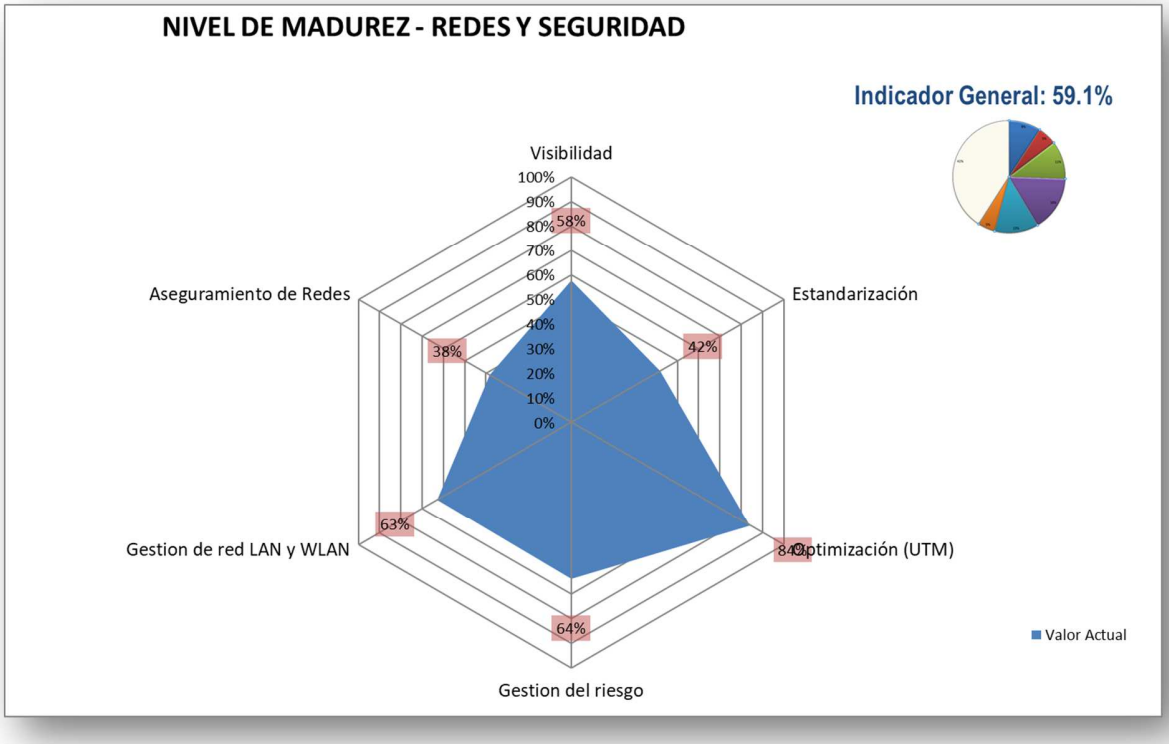


Gráfico 16 Calificación del análisis de Madurez

Indicadores Generales

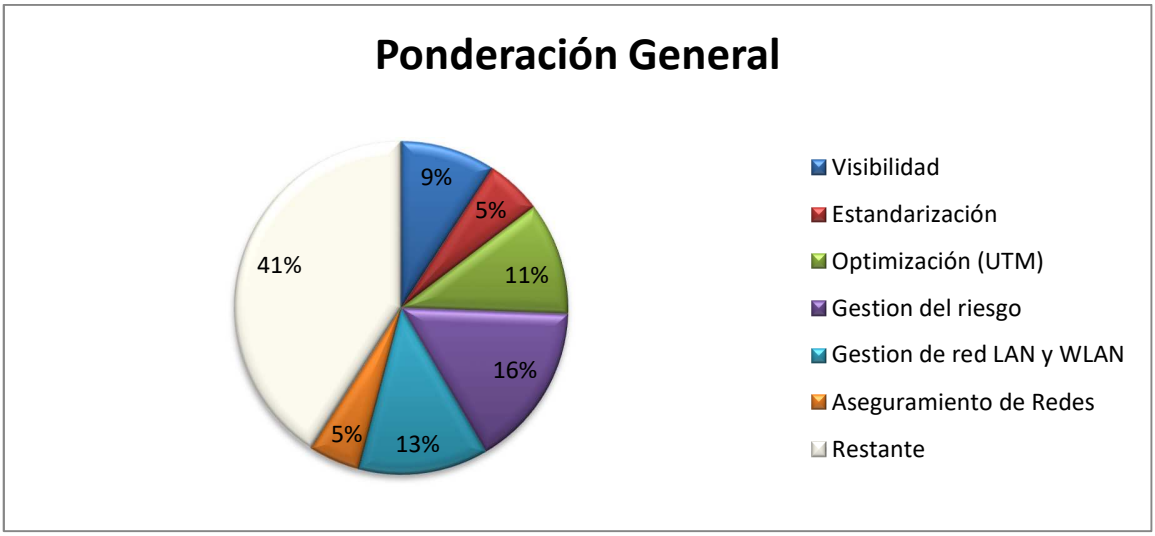


Gráfico 17 Ponderación General

Peso General	Ponderación	Categoría	Ponderación General
16%	58%	Visibilidad	9,2%
13%	42%	Estandarización	5,4%
13%	84%	Optimización (UTM)	10,9%
25%	64%	Gestión del riesgo	16,0%
20%	63%	Gestion de red LAN y WLAN	12,6%
13%	38%	Aseguramiento de Redes	5,0%
		Nivel de Madurez	**59,1%**

Tabla 2.. Resultados Análisis de Madurez

Con los datos anteriores, se puede determinar, que la empresa persenta mayores falencias en los campos de Aseguramiento de redes y estandarización, por lo cual se debe empezar a trabajar de manera prioritaria en los ítems de cada una de estas categorías que presentan un bajo nivel de avance.

Finalmente, con motivo de tener visibilidad y poder comparar si realmente se ha avanzado en cuando a mejorar un nivel de madurez de la seguridad de la información, se recomienda realizar este análisis en un período no mayor a seis (6) meses.

Análisis de vulnerabilidades

Para llevar a cabo el análisis de vulnerabilidades de la red de empleados y servidores de Servicios TI, con el fin de analizar aspectos críticos en la infraestructura de las plataformas de las Tecnologías de la empresa y potenciales falencias relacionadas al Ransomware, se utilizaron las siguientes herramientas en versiones libres o por períodos de prueba:

- Nessus Professional Vulnerability Scanner, de la empresa (Tenable)
- Acunetix Web Site Vulnerability Scanner, de la empresa (Acunetix)
- Nexpose Vulnerability Management, de la empresa (Rapid7)
- Metasploit Framework Penetration and Testing Software, de la empresa (Metasploit)
- Nmap Network Mapper, Free Security Scanner, Proyecto GLP (Software Libre y abierto).
- Qualys Vulnerabilities Assesment, de la empresa (Qualys)

Es escaneo de vulnerabilidades se aplicó a los siguientes objetivos en la red corporativa:

- Red de equipos de servidores.
- Red de usuario final.

- Servicios WEB publicados en Internet.

Vale la pena resaltar, que la red de clientes y servidores comparten el mismo direccionamiento IP, lo cual no es una buena práctica, debido a que los servidores comparten un mismo dominio de difusión (Broadcast), que los equipos de usuario final y en caso de que un equipo cliente llegase a ser infectado con alguna amenaza tipo Botnet o Ransomware, esta podría llegar a la red de servidores de una manera más directa.

Vulnerabilidades encontradas en la red

En el análisis de vulnerabilidades a la red de servidores y clientes, se escanearon diferentes objetivos, tales como:

- Sistemas Operativos de Servidores (Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 y Linux CentOS).
- Sistemas Operativos de usuario final (Windows 7, Windows 10, MacOS).
- Firmware de los sistemas de almacenamiento.
- Servicios web publicados.

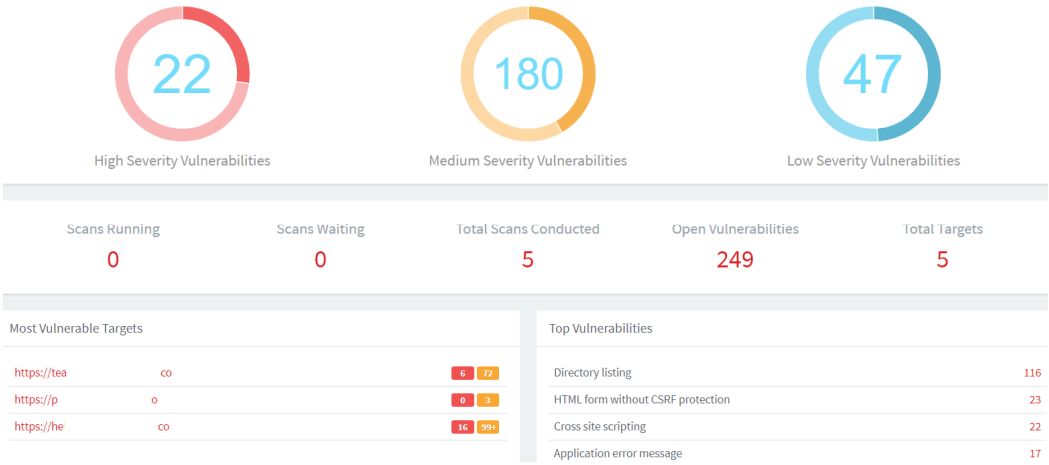


Gráfico 18. Resumen de las amenazas encontradas

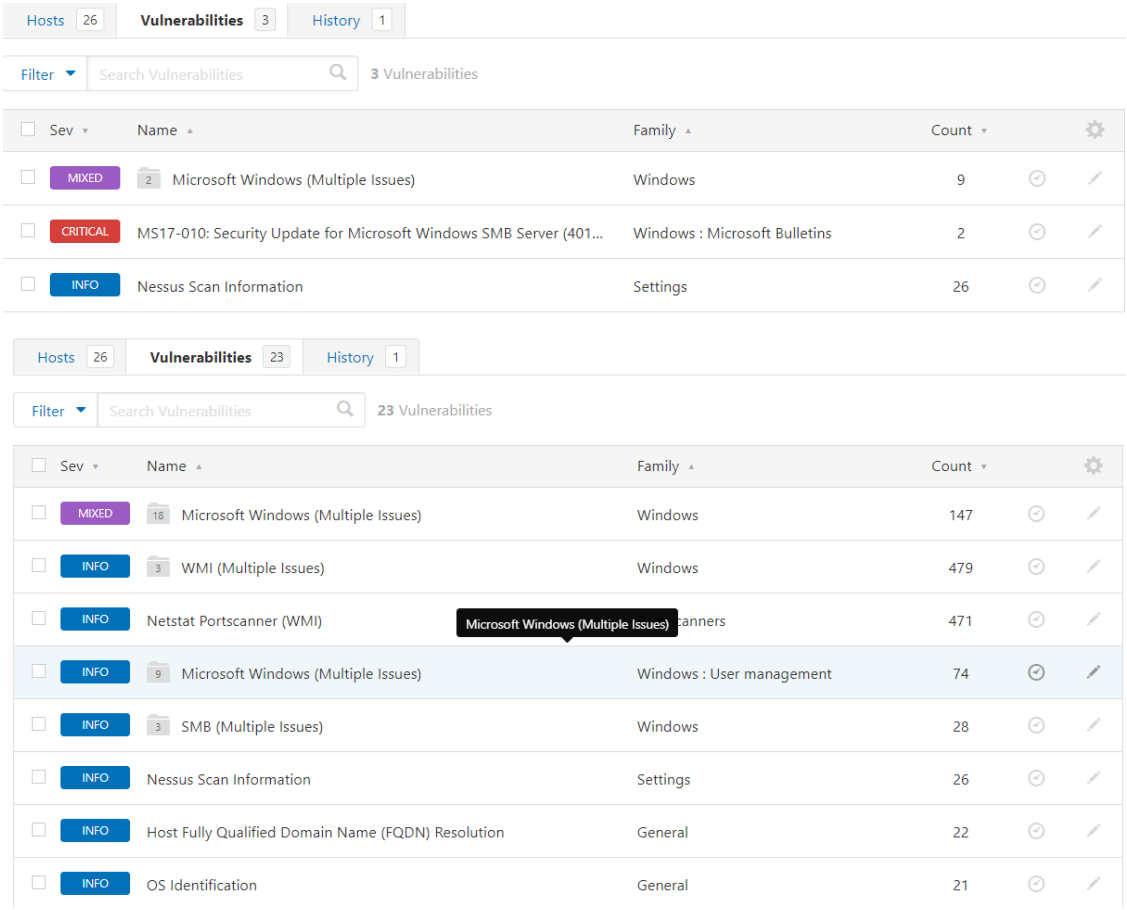


Gráfico 19. Resumen del análisis con Nessus

Como se puede observar en la información anterior, se encontraron vulnerabilidades las cuales se encuentran categorizadas con diferentes calificaciones por parte de la herramienta de análisis de vulnerabilidades “Nessus”:

Categoría del Riesgo	Descriptor	Descripción
5	**Crítica**	Requiere acción inmediata
4	**Alta**	Debe considerar una acción y un plan de contingencia
3	**Media**	Debe considerar ejecutar una acción
2	**Baja**	Necesaria una revisión periódica
1	**Información**	Impacto trivial

Tabla3. Categorización del riesgo

Dentro de las principales vulnerabilidades encontradas, se encuentran algunas tales con SMB versión 1 o también llamada (Ethernal Blue), versiones obsoletas e inseguras de PHP MyAdmin, divulgación de información tales como versiones de sistemas operativos o versiones de software, listado de directorios, entre otras.

La vulnerabilidad de SMBv1, es utilizada por amenazas de ciberseguridad tales como el Ransomware, tal como lo informa (Microsoft, 2017), “El ransomware WannaCrypt está aprovechando una de las vulnerabilidades que la actualización MS17-

010 aborda. Los equipos que no tienen MS17-010 instalado sufren un riesgo mayor debido a que existen varias cepas de este malware".

A continuación, se muestra las vulnerabilidades asociadas a SMBv1, encontradas por el scanner de vulnerabilidades "Nessus", las cuales son necesarias revisar y remediar lo más pronto posible, debido a la gravedad que implican para la seguridad de estos recursos y otros que se encuentren en la misma red de comunicaciones:

Servidor CAOS

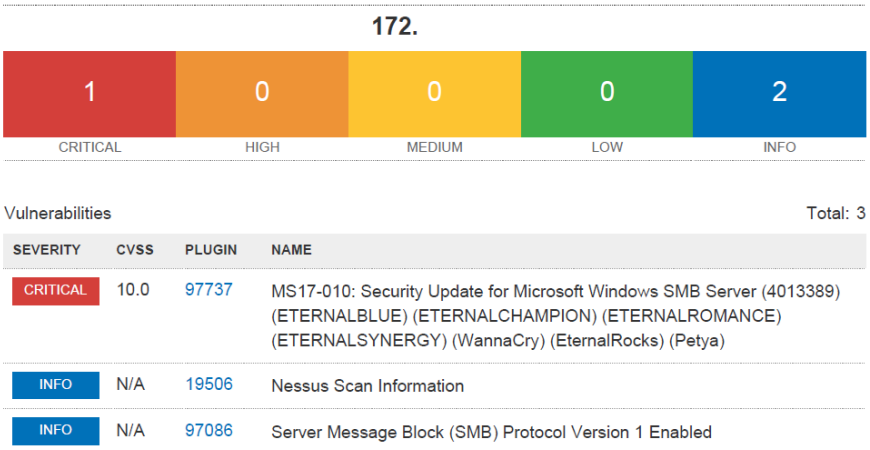


Gráfico 20. Análisis de Ransomware a Servidor CAOS

Servidor HEFESTOS

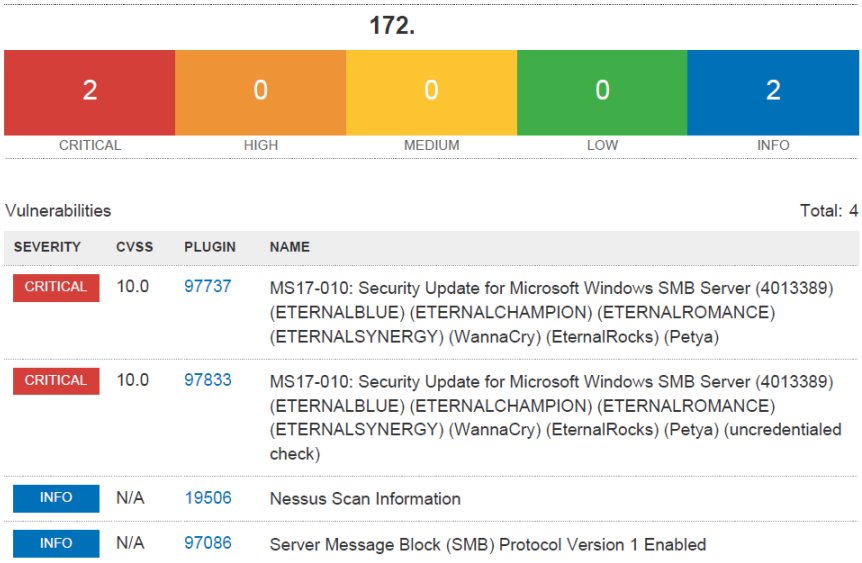


Gráfico 21. Análisis de Ransomware a Servidor HEFESTOS

En el análisis, también se encontraron varios servidores que tienen la versión de 1 de SMB de Microsoft activa y aunque el sistema operativo cuenta con parches asociados a esta versión, Microsoft recomienda desactivar esta versión y trabajar con la versión 2 de este protocolo. Los servidores que se encontraron con SMBv1 activo, fueron los siguientes:

Servidor HERA

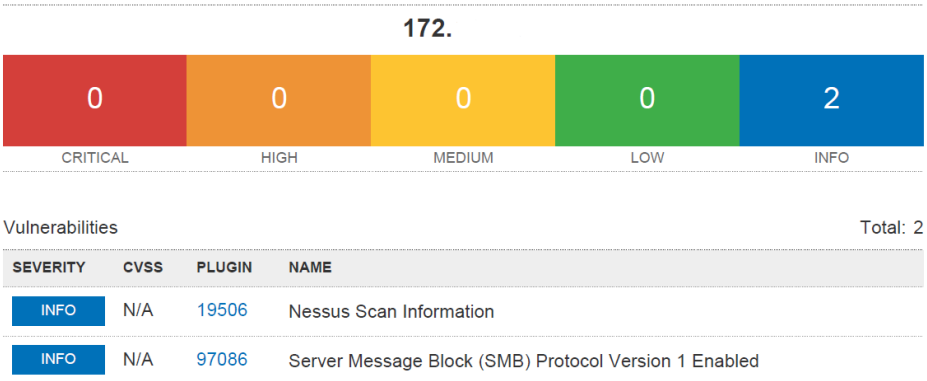


Gráfico 22. Análisis de Ransomware y SMB V1 de servidor HERA

Servidor CERBERUS

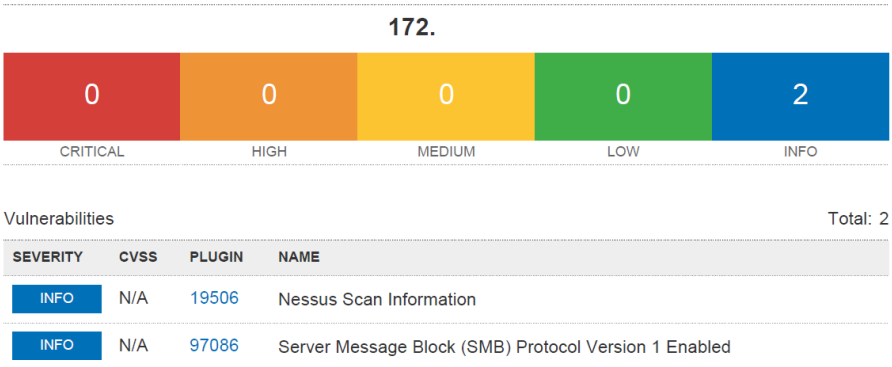


Gráfico 23. Análisis de Ransomware y SMB V1 de servidor CERBERUS

Servidor CAOS

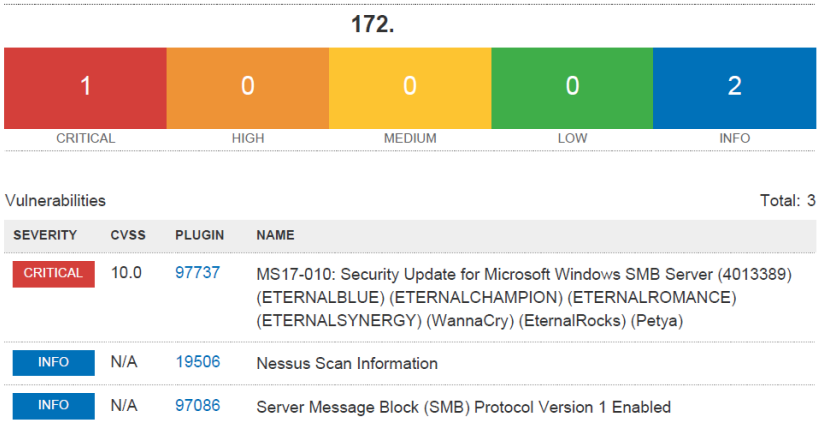


Gráfico 24. Análisis de Ransomware y SMB V1 de servidor CAOS

Servidor HADES

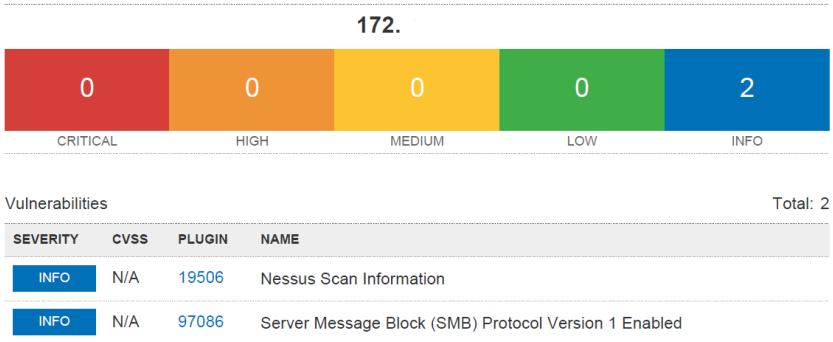


Gráfico 25. Análisis de Ransomware y SMB V1 de servidor HADES

Servidor HERMES

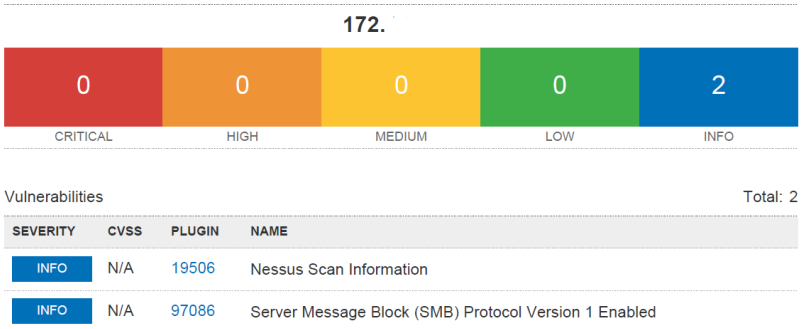


Gráfico 26. Análisis de Ransomware y SMB V1 de servidor HERMES

Servidor HEFESTOS

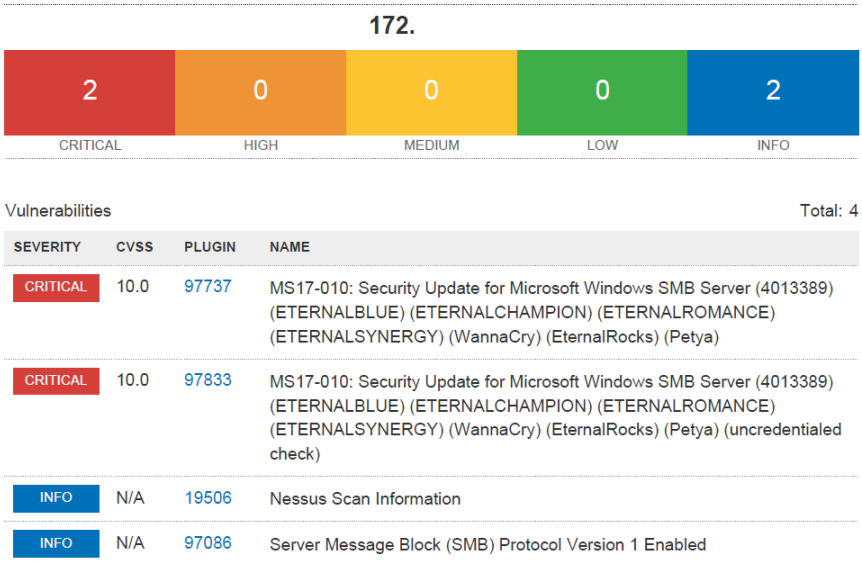


Gráfico 27. Análisis de Ransomware y SMB V1 de servidor HEFESTOS

Servidor URANO

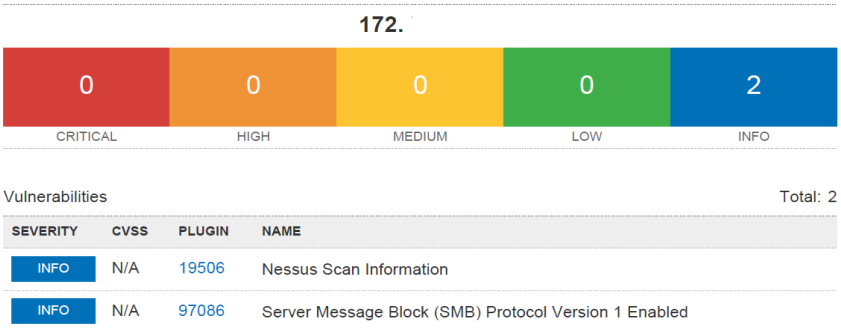


Gráfico 28. Análisis de Ransomware y SMB V1 de servidor URANO

Servidor ZEUS

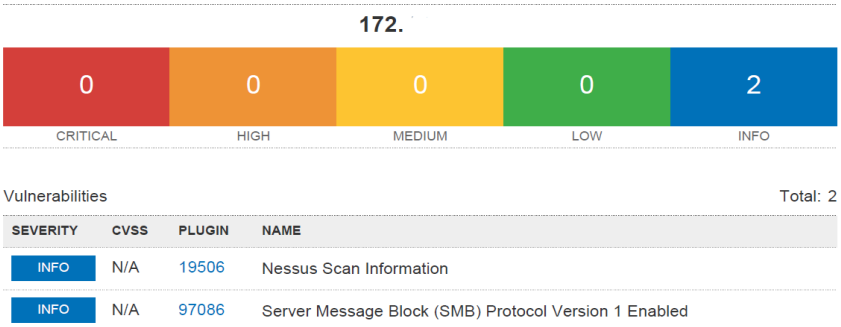


Gráfico 29. Análisis de Ransomware y SMB V1 de servidor ZEUS

Adicional al escáner realizado a la granja de servidores productivos de la compañía con la herramienta Nessus, también se hizo un escáner de la red con la herramienta "Metasploit Framework" y haciendo uso de su Payload o programa auxiliar "SMB_MS17_010", se encontraron 3 equipos de usuario final en la red, los cuales presentan la vulnerabilidad de SMBv1, los cuales se muestran a continuación:

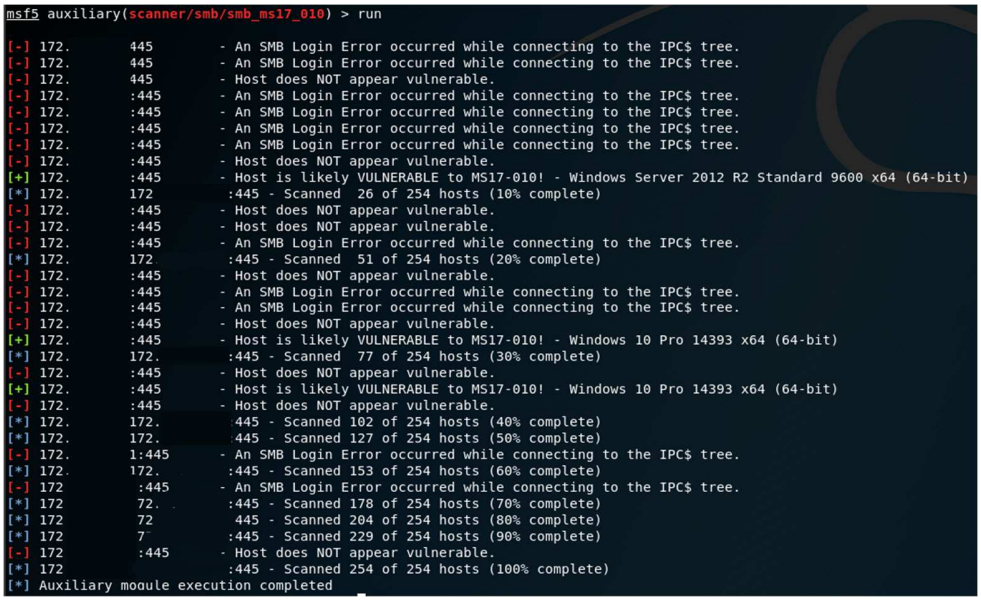


Gráfico 30. Análisis de vulnerbilidades con MetaSploit

Otro de los análisis que se realizaron con las diferentes herramientas, fue hacia los sitios WEB publicados por la empresa Servicios TI, de los cuales se encontraron diferentes tipos de vulnerabilidades en diferentes categorías de gravedad. A continuación, se muestran las vulnerabilidades encontradas por el scanner de vulnerabilidades “Acunetix”, en el servidor de Mesa de Ayuda.

Vulnerabilities

Scan details

Scan information		
Start url	https://	.com
Host	https:/	.com

Threat level

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	154
High	16
Medium	105
Low	20
Informational	13

Gráfico 31. Resumen de amenazas encontradas por Acunetix

El análisis al servidor que almacena credenciales y accesos también presenta un número importante de vulnerabilidades y algunas de estas son críticas:

Vulnerabilities

Scan details

Scan information		
Start url	https:/	.com
Host	https:/	.com

Threat level

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	119
High	6
Medium	72
Low	12
Informational	29

Gráfico 32. Resumen de amenazas encontradas por Acunetix

Adicional al anterior análisis, también se realizó un análisis de vulnerabilidades a los servicios de mesa de ayuda y correo de la compañía publicados, con la solución de

seguridad “Qualys”, el cual arrojó varias brechas de seguridad con severidad alta, media y baja, las cuales son recomendables remediar prontamente.

Vulnerabilidades críticas encontradas al servidor de mesa de ayuda, con la herramienta Qualys.

Gráfico 33. Vulnerabilidades críticas del servidor 1

Vulnerabilidades intermedias encontradas al servidor de mesa de ayuda, con la herramienta Qualys.

Gráfico 34. Vulnerabilidades intermedias del servidor de Mesa de Ayuda

Las siguientes, son las vulnerabilidades de seguridad encontradas al servidor de correo de la compañía, las cuales presentan un alto riesgo para la integridad y confidencialidad de la información, debido a que algunas de estas son explotables por personas con conocimientos intermedios sobre seguridad informática.

Como se puede observar, la mayoría de estas vulnerabilidades hacen referencia al certificado SSL, por lo cual es necesario revisarlo y si actualmente se encuentra "Auto-Firmado", se recomienda configurar un certificado firmado por una entidad certificadora.

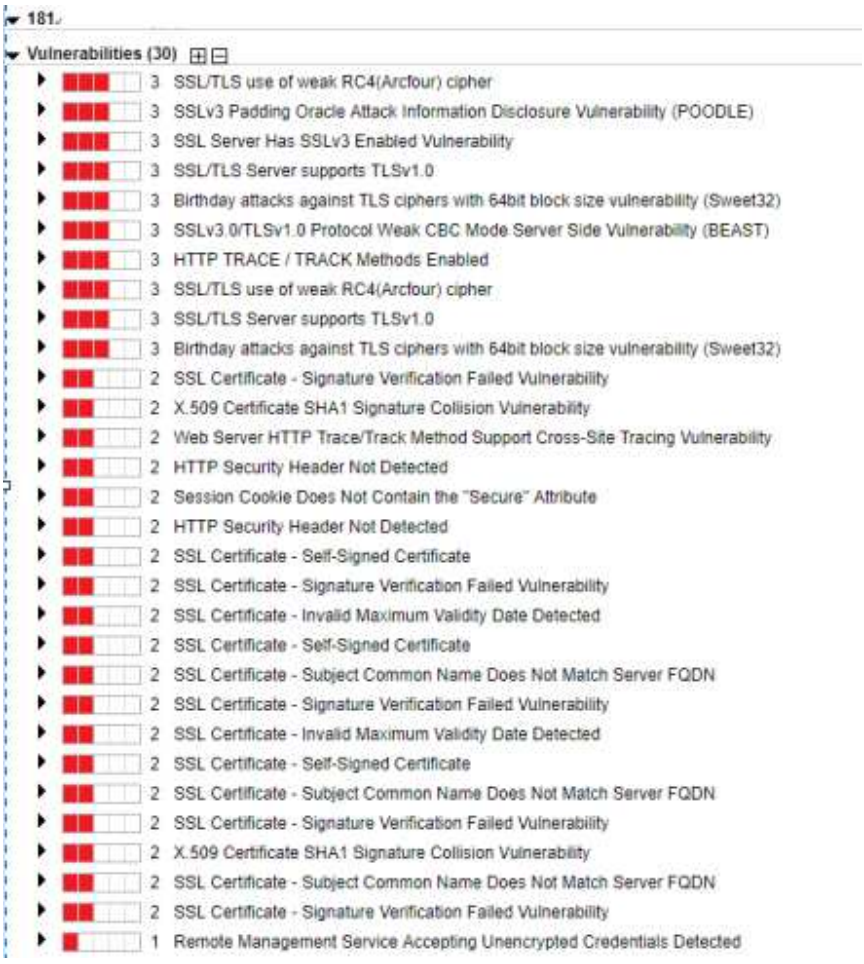


Gráfico 35. Resumen de amenazas encontradas con Acunetix

Las que se muestran a continuación, son las vulnerabilidades de un grado intermedio, encontradas a la publicación del servidor de correo:

Gráfico 36. Vulnerabilidades Intermedias del servidor 2

Cabe resaltar que del análisis que se realizó con la herramienta Qualys a los servicios de la mesa de ayuda y correo, no se decidió compartir las vulnerabilidades con nivel bajo o informativas, debido a que se compartirán en el informe técnico a la dirección de servicios de Servicios TI.

A continuación, se presenta el detalle de las vulnerabilidades encontradas con las diferentes herramientas, la cantidad, servicios afectados, riesgos, impactos, evidencias, maneras de remediar la vulnerabilidad y enlaces a sitios de empresas expertas en seguridad

de la información, para tener información adicional sobre las brechas de seguridad encontradas.

Vulnerabilidad: MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya)
Referencias: EthernalBlue, Ethernalromance CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148
Número de Vulnerabilidades Identificadas: 3
Servicios- Items Afectados: Servidor CAOS, HEFESTOS Puerto TCP 137, 139 y 445 Puerto UDP 137/138
Descripción de la Vulnerabilidad: Esta vulnerabilidad en Microsoft Windows es considerada por Microsoft de las más graves, debido a que podría permitir la ejecución remota de código si un atacante envía mensajes especialmente diseñados a un servidor de Microsoft Server Message Block 1.0 (SMBv1). ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE y ETERNALSYNERGY son cuatro de los múltiples vulnerabilidades y explotaciones de Equation Group. Se divulgaron el 2017/04/14 por un grupo conocido como Shadow Brokers. WannaCry / WannaCrypt es un programa de ransomware que utiliza el exploit ETERNALBLUE y EternalRocks, un gusano que utiliza siete vulnerabilidades del Grupo Equation. Petya es un programa de ransomware que primero utiliza CVE-2017-0199, una vulnerabilidad en Microsoft Office, y luego se propaga a través de ETERNALBLUE.
Detalles de la Vulnerabilidad: Esta vulnerabilidad afecta a cualquier sistema operativo Microsoft que tenga activo el protocolo SMBv1 y que no tenga instalado el parche de seguridad “MS17-010”.
Factor de Riesgo: Crítico • Un atacante que explotó con éxito las vulnerabilidades podría obtener la capacidad de ejecutar código en el servidor de destino.

- Para aprovechar la vulnerabilidad, en la mayoría de las situaciones, un atacante no autenticado podría enviar un paquete especialmente diseñado a un servidor SMBv1 específico.

- Infección de malware tipo Ransomware, debido a que estas variantes, utilizan este protocolo para propagarse en la red.

Impacto:

- Secuestro de información valiosa para la continuidad del negocio.
- Indisponibilidad de servicios críticos para la compañía.
- Pérdida de la integridad y confidencialidad del servidor que contiene al sitio web de la mesa de servicios, ya que un ciberdelincuente, puede tomar el control parcial o total del servidor.

Evidencias:

Recomendación para solucionar esta Vulnerabilidad:

- Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, y 2016. Microsoft también ha lanzado parches de emergencia para sistemas operativos Windows que ya no son compatibles, incluyendo Windows XP, 2003 y 8.

Referencias Web:

https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010
http://www.nessus.org/u?321523eb
http://www.nessus.org/u?065561d0
http://www.nessus.org/u?d9f569cf
https://github.com/stamparm/EternalRocks/
http://www.nessus.org/u?59db5b5b

Observaciones:

El malware para atacar esta vulnerabilidad, puede ser descargado fácilmente desde foros, proyectos de GitHub o utilizando software de CANVAS, Core Impact o Metasploit.

Vulnerabilidad:
Server Message Block (SMB) Protocol Version 1 Enabled

Referencias:
CVE-2017-0271

Numero de Vulnerabilidades Identificadas: 8

Servicios- Items Afectados:
Servidor HERA
Servidor CERBERUS
Servidor CAOS
Servidor HADES
Servidor HERMES
Servidor HEFESTOS
Servidor URANO
Servidor ZEUS

Puerto TCP 137, 139 y 445
Puerto UDP 137/138

Descripción de la Vulnerabilidad:

El host remoto de Windows admite Server Message Block Protocol versión 1 (SMBv1). Microsoft recomienda Que los usuarios interrumpan el uso de SMBv1 debido a la falta de funciones de seguridad que se incluyeron en SMB posteriores.
Además, el grupo de Shadow Brokers tiene un exploit que afecta a SMB. US-CERT recomienda que el usuario deshabilite SMBv1 según las mejores prácticas de SMB para mitigar estos problemas potenciales.

Detalles de la Vulnerabilidad:

Esta vulnerabilidad afecta a cualquier sistema operativo Microsoft que tenga activo el protocolo SMBv1 y que no tenga instalado el parche de seguridad “MS17-010”.

Factor de Riesgo: Bajo (Parcial)

- Es considerado como divulgación de información (Puertos y versiones del protocolo).
- Si un atacante conoce la versión del protocolo, puede intentar utilizar técnicas de explotación para logar tener acceso al sistema.
- No se requiere autenticación para explotar esta vulnerabilidad.

Impacto:

- Un ciberdelincuente podría obtener información sobre la versión del protocolo de SMB y podría utilizar técnicas para explotar este, si se encuentra desactualizado.
- En caso de explotar la vulnerabilidad, el atacante podría ejecutar código arbitrariamente, en el equipo víctima.

Evidencias:

Recomendación para solucionar esta Vulnerabilidad:

- Deshabilite SMBv1 de acuerdo con las instrucciones del proveedor en Microsoft KB2696547. Además, bloquee SMB directamente bloqueando el puerto TCP 445 en todos los dispositivos de Firewall de red. Para SMB sobre la API de NetBIOS, bloquee los puertos TCP 137/139 y los puertos UDP 137/138 en todos los dispositivos de Firewall de red.

Referencias Web:

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/
https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and
http://www.nessus.org/u?8dcab5e4
http://www.nessus.org/u?234f8ef8
http://www.nessus.org/u?4c7e0cf3

Observaciones:

Esta versión de SMB, puede ser explotada con varios payloads de Metasploit Framework, por personas con conocimientos de seguridad intermedios.

Ingeniería social

Con el fin de determinar el nivel de conocimiento de los empleados de la empresa "Servicios TI" referente a las nuevas amenazas de seguridad de la información tales como Ransomware y la manera en que estas pueden ingresar y afectar información sensible para la continuidad de la compañía, se realizaron pruebas de Ingeniería social, lo cual es una práctica para "manipular" psicológicamente a los usuarios, con el fin de que compartan información confidencial, brinden credenciales de acceso, abran enlaces a sitios fraudulentos o realicen como tal acciones inseguras dentro de la red de una empresa o en sus entornos personales.

Para este caso, se utilizó como vector de ataque (falencia o falla de seguridad que permite iniciar un ataque), el correo electrónico corporativo de la compañía "Servicios TI", al cuál se estará enviando a un total de 20 cuentas aleatoriamente, por medio de una herramienta de de generación de SPAM (Correo basura) y Phishig (Suplantación de identidad por correo electrónico), un correo similar a los que envían proveedores de la empresa pero falsificado, el cual los lleve a un enlace que simula una infección de Ransomware en el computador. Esto se hace con el fin de determinar si el personal administrativo de la compañía conoce de fundamentos sobre la seguridad de los datos, si piden ayuda al personal de servicios tecnológicos de la compañía o si por el contrario deciden abrir el mensaje con el enlace fraudulento.

Configuración del Phishing

Para llevar a cabo este ataque, se utilizó la herramienta gratuita en linea llamada "Emkei's Mail Failer", cuya dirección es la siguiente: "https://emkei.cz", la cual permite enviar un correo electrónico anónimo o desde un dominio similar a uno exixtente hacia cualquier cuenta de correo de cualquier dominio.

Vale la pena resaltar que no es posible enviar un correo electrónico desde por ejemplo el dominio @uniminuto.edu, debido a que existe actualmente, pero si se puede enviar un mensaje desde cualquier cuenta del dominio @uniminuto.com.edu debido a que este no ha sido adquirido y/o registrado por la institución.

La interfaz del sitio es muy simple, inclusive es muy similar a un cliente de correo normal, debido a que solicita los mismos campos para realizar el envío del mensaje. Para poder ingresar al sitio, es necesario un navegador Web, tal como Mozilla Firefox, Google Chrome, Opera Browser o Safari y está desarrollado en HTML5, por lo cual no es necesario instalar algún complemento para trabajar en el mismo.

La interfaz del sitio es la siguiente:

Gráfico 36. Interfaz de Ermkei's Mailer

A continuación se ilustra el procedimiento que se utilizó para enviar a las 20 cuentas de correo electrónico de la empresa "Servicios TI", el correo "malicioso" similiar al de un proveedor de servicios de la compañía, el cual contiene embebido un enlace, para que al momento de abrirlo simule una infección por Ransomware, la cual trabaja del mismo modo en caso de una infección por Malware real.

Nota: Por motivos de privacidad del proveedor de la compañía, se reemplazará la imagen que se envió a los colaboradores de "Servicios TI", nombre de la empresa y dirección de correo por un correo similar al dominio de Microsoft.

Los campos a completar para enviar el correo fraudulento son los siguientes:

- **Fron Name:** Nombre que desea que se visualice en el campo de remitente.
- **From E-mail:** Cuenta de correo del remitente, en este caso hemos inventado una dirección de correo “support@microsoft.com.gov”.
- **To:** Cuenta de correo del destinatario.
- **Subject:** Asunto del correo electrónico.
- **Content- Type:** Se debe seleccionar la opción “Text/HTML” y seguido la opción Editor.
- **Add Image:** En el ícono de la imagen, se deberá copiar una direcciónen la cual se encuentre almacenada la imagen que se desea enviar como cuerpo del correo.
- **Add Link:** Es en el campo, en el cuál se anexará un enlace a un sitio que simula una infección por Ransomware. Este sitio se abrirá al momento de dar clic en la imagen anexada en el punto anterior.

El resto del trabajo solamente dependerá de la creatividad del atacante, debido a que, si se conocen los intereses del objetivo, clientes, proveedores o temas de interés, éste se verá tentado a abrir el enlace. El correo que se envió a los colaboradores de “Servicios TI”, estaba asociado a una invitación a un evento que realiza periódicamente uno de los proveedores de la compañía al personal del área comercial.

A continuación, se muestra como quedó el mensaje de correo electrónico, el cual se enviará al objetivo. Como se explicó previamente, en este ejemplo no se muestran datos del proveedor real, por temas de confindencialidad.

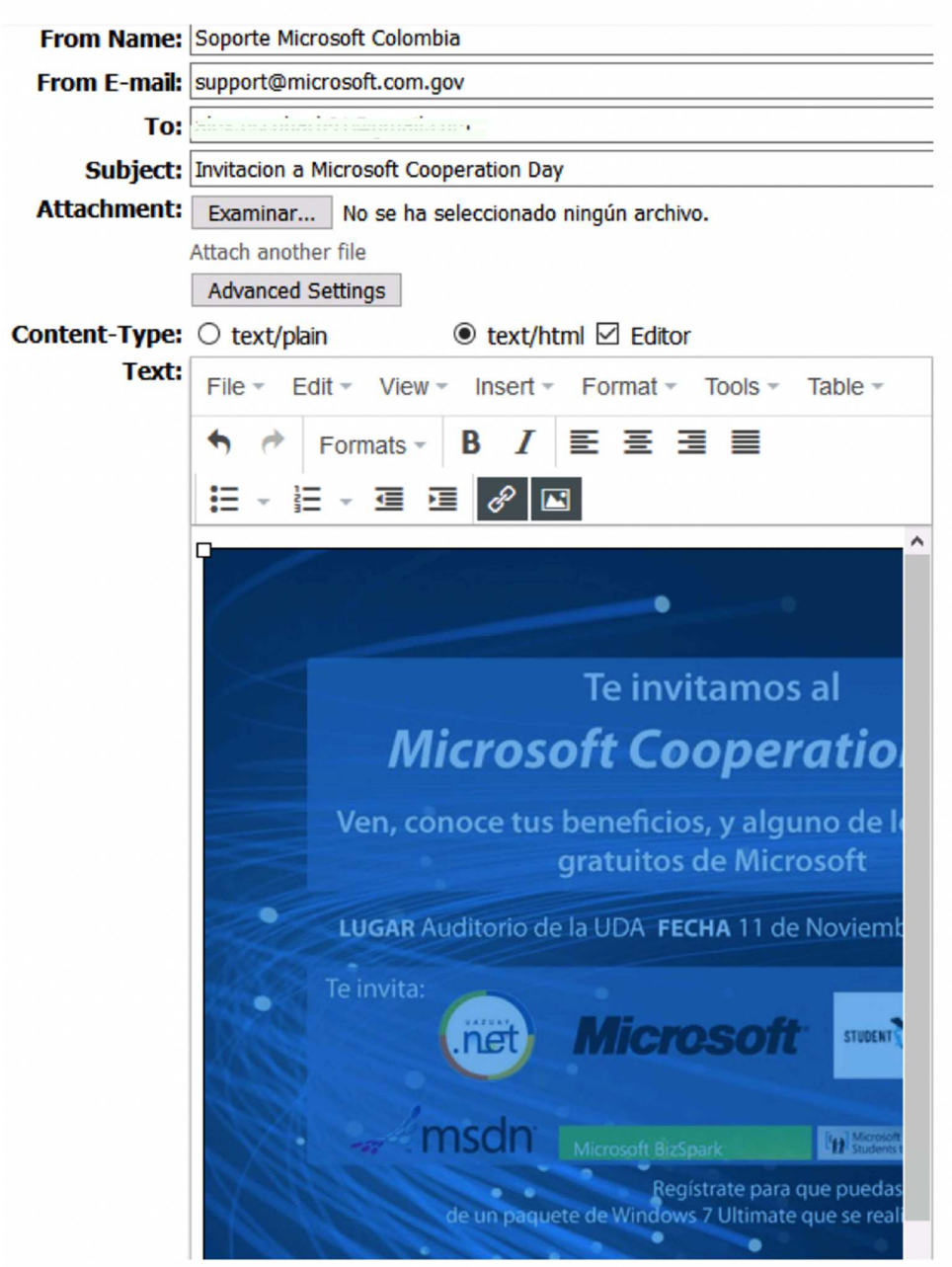


Gráfico 37. Configuración del Phishing

Las víctimas del correo fraudulento, estarán recibiendo en su bendeja de entrada, un correo con la información suministrada en los pasos anteriores y al abrir este lo podrán visualizar como un correo real.

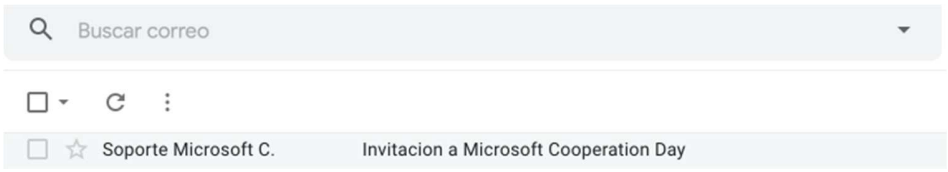


Gráfico 38. Bandeja de entrada del correo Phishing

Nota: Inicialmente, el correo fue bloqueado por el sistema "AntiSpam" de la empresa, pero con el fin de conocer el comportamiento de los usuarios al recibir este tipo de información, con autorización del gerente de servicios de "Servicios TI", se procede habilitando en listas clancas, el dominio "@microsoft.com.gov".

La siguiente es la información que los usuarios víctimas, estarán recibiendo al correo electrónico:

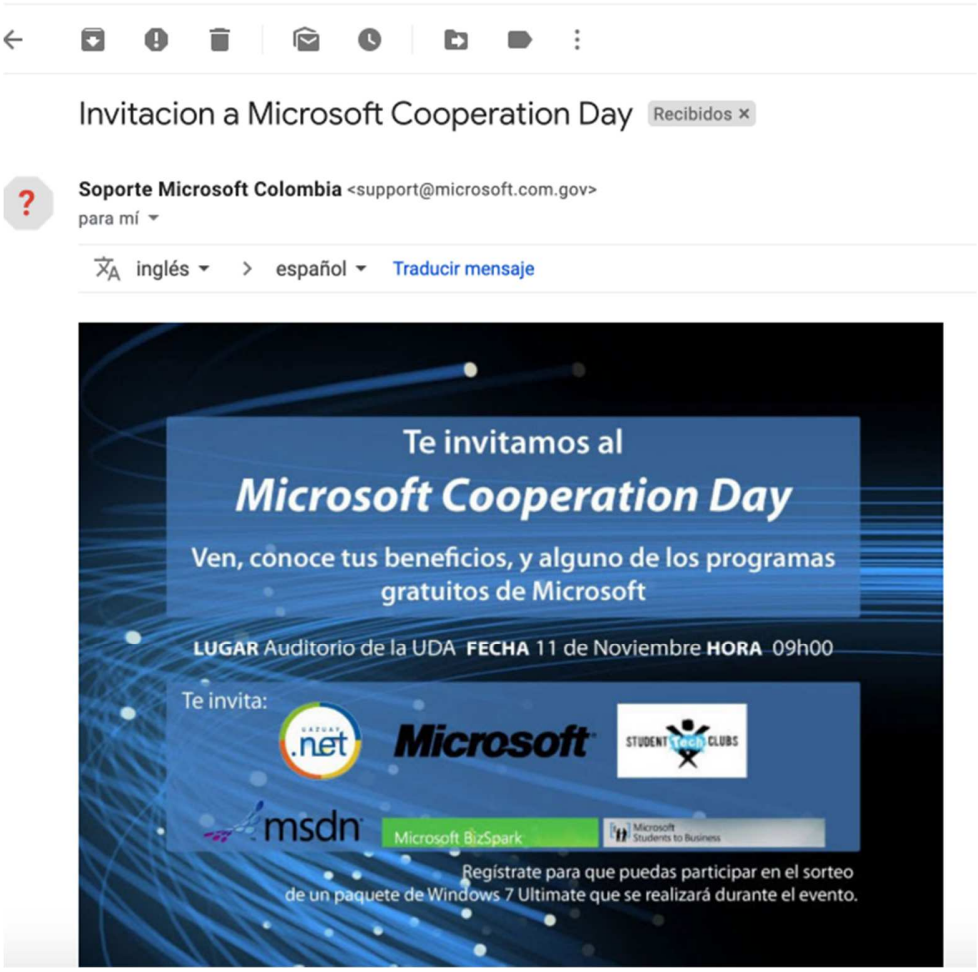


Gráfico 39. Visualización del correo malicioso

Al momento de dar clic en la imágen, inmediatamente se abrirá un enlace con un sitio que simula una infección por Ransomware, exigiendo un rescate por la "liberación" de estos archivos. El enlace original para el sitio que simula una infección por

Ransomware, es el siguiente: https://www.cryptoprank.com, pero con el fin de que el usuario no sospeche que es un enlace desconocido, se utiliza un servicio de acortador de enlaces, el cual cifra esta URL y con esto, la víctima, no sabrá realmente cual es el destino del enlace. El enlace acortado es https://bit.ly/2qmSPnt.

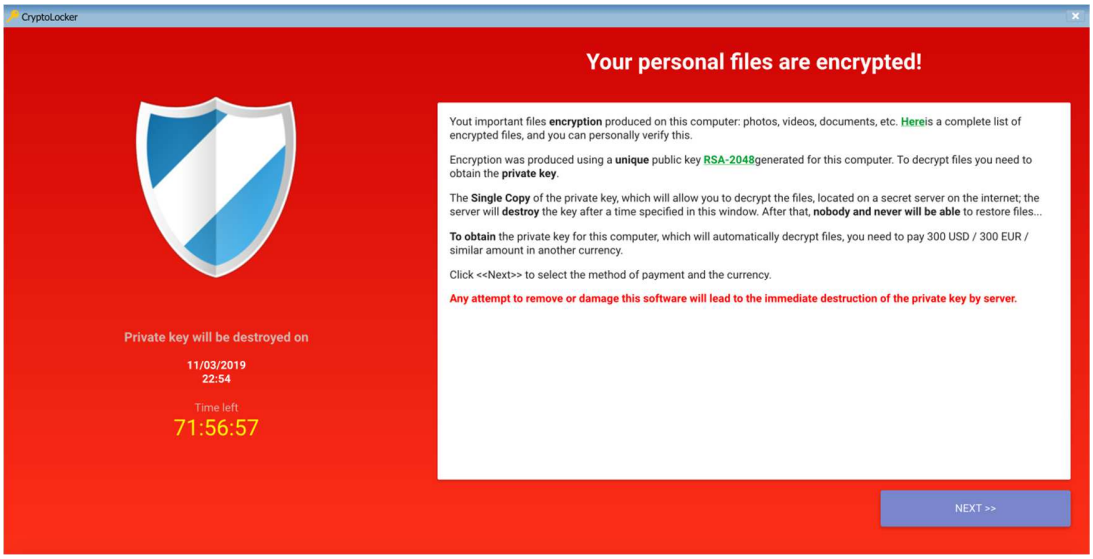


Gráfico 40. Simulación de infección por Ransomware

Como se explicó previamente, este es solo un ejemplo ilustrativo, pero de este mismo modo, se puede enviar un enlace que contenga un Script con una infección de Ransomware y afectar información sensible para la empresa.

Estadísticas de la prueba

Para realizar la prueba, se tomaron aleatoriamente veinte (20) cuentas de usuarios de diferentes áreas de la compañía, obteniendo como resultado que siete (7) usuarios abrieron el enlace e informaron al personal de TI e informaron posteriormente de la acción realizada, once (11) personas decidieron omitir el correo y solamente dos (2) lo reportaron al personal de sistemas de la compañía.

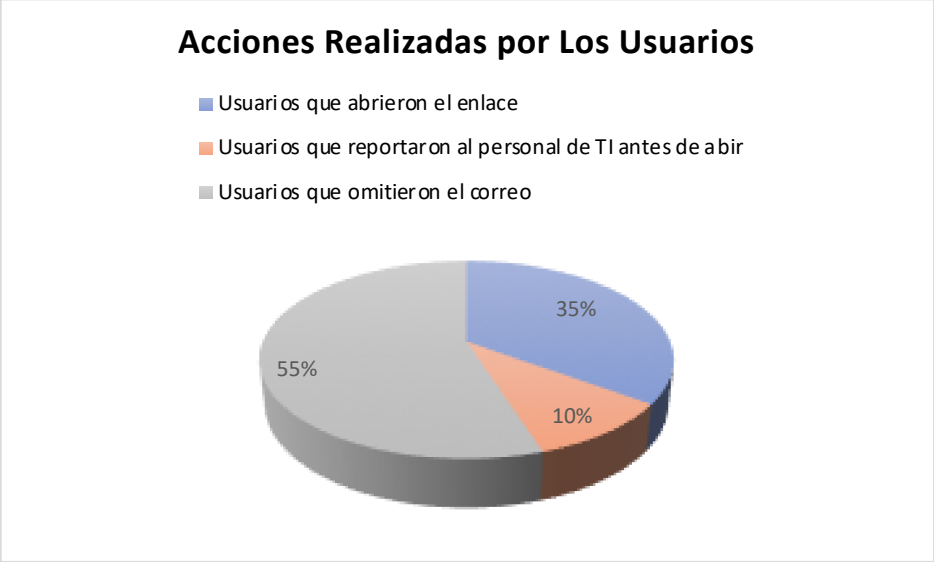


Gráfico 41. Estadísticas de las acciones realizadas por los usuarios de Servicios TI

La cifra anterior, refleja una preocupante situación, debido a que la mayoría de los usuarios no informaron al personal de informática de la empresa, porque no supieron identificar que el correo electrónico no provenía de una cuenta oficial de un proveedor de servicios y contenía un contenido no deseado. Con base a esto, se crearán tips de seguridad, con el fin de concientizar sobre los riesgos a los cuales se enfrentan a diario al momento

de trabajar con herramientas tecnológicas, tales como correo electrónico, sitios Web, bases de datos, compras por Internet, instalación de Aplicaciones, entre otros.

Métodos de Defensa

Como se pudo observar previamente, para realizar esta técnica de ataque, no es requerido mucho conocimiento sobre informática, simplemente con indagar un poco en Internet, cualquier usuario puede hacerlo y este es simplemente un vector de ataque por los cuales se puede propagar un Ransomware en una red corporativa.

Entrando en el análisis de caso práctico, se debe reconocer que la empresa "Servicios TI", tiene implementado un buen dispositivo de seguridad para impedir que el correo malicioso o no deseado, llegue a las cuentas de correo de sus usuarios, por lo cual fue necesario agregar el dominio "microsoft.com.gov" a sus listas de excepciones. No obstante, los usuarios pueden recibir este enlace por diferentes medios, como por ejemplo a un correo personal el cual abran desde los equipos corporativos o en equipos personales que estén conectados a la red de la empresa.

Unas de las claves para que los usuarios lograran reconocer que este era un correo malicioso, era el dominio desde el cual se envió debido a que el de la empresa Microsoft es "@microsoft.com" y el que se creó con fines educativos fue "@microsoft.com.gov". Adicionalmente, si no se conoce el destino de la URL que contiene una imagen, basta con

dar clic derecho a esta y presionar la opción “Copiar la ruta del enlace” para verificar hacia que lugar quiere redirigirlo el remitente del correo.

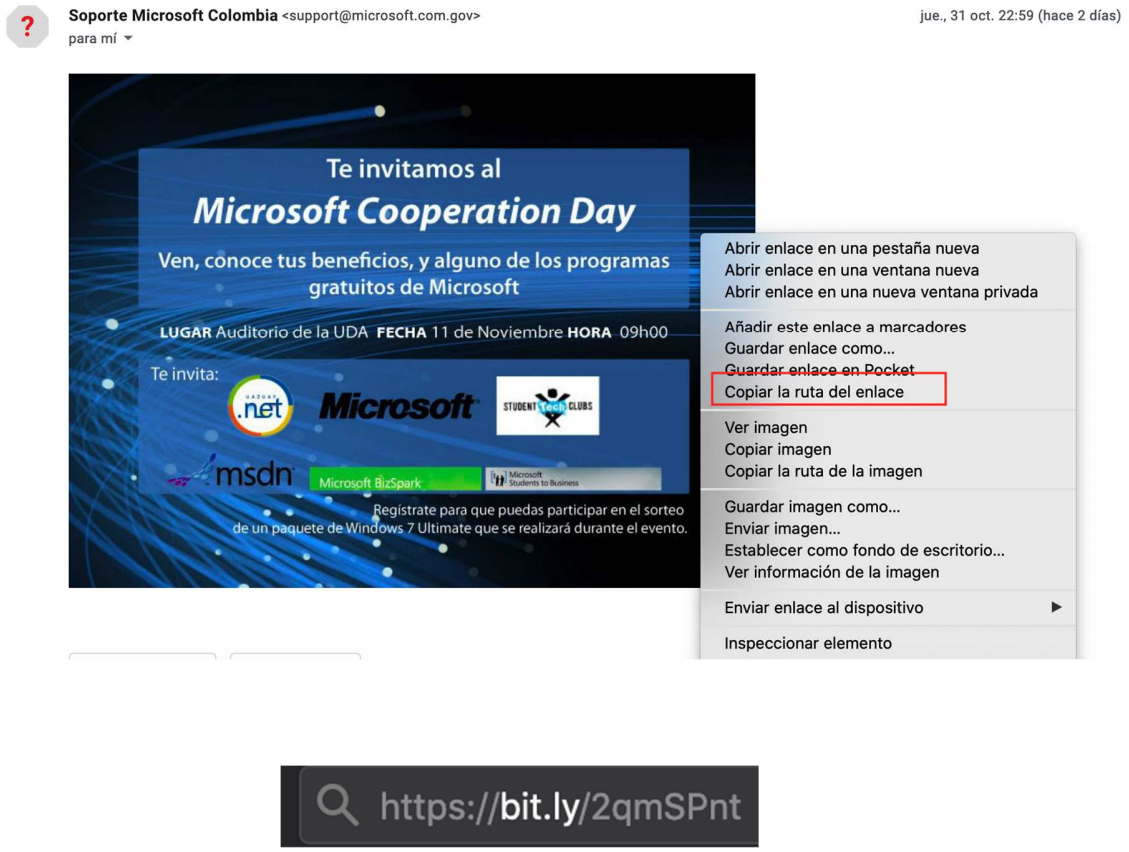


Gráfico 42. Verificación de enlace malicioso

En este caso la URL a la cual se redirige es la que se había mencionado, la cual esta modificada por un acortador de enlaces, por lo cual ya es un indicio de que no es un correo seguro. Normalmente que se envía enlace hacia contenido a externos, son páginas conocidad o del mismo dominio desde se envió el mensaje.

Finalmente, otro aspecto y muy importante al que los usuarios que abrieron el mensaje hicieron caso omiso, fue la notificación del cliente de correo electrónico

informando que el enlace al cual se quiere acceder está categorizado como sospechoso y que si desea acceder a este. Por lo cual como una medida de prevención el personal de "Servicios TI" no debió haber abierto el mensaje. A continueación se muestra la notificación de advertencia sobre el sitio próximo a ser abierto.

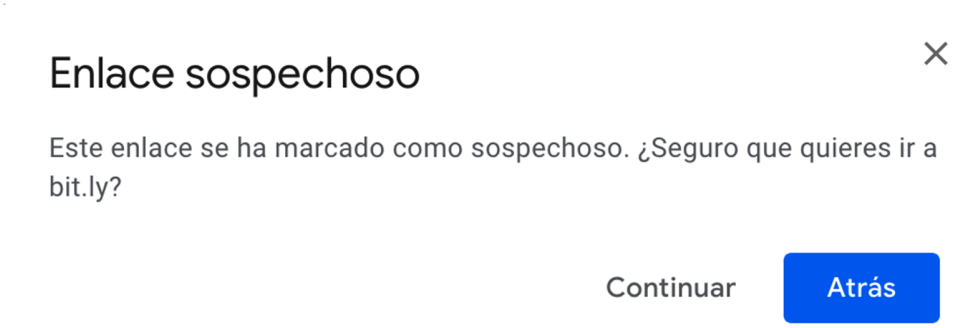


Gráfico 43. Advertencia del cliente de correo

Remediaciones

Con el objetivo de solucionar las vulnerabilidades seguridad encontradas en los servidores, dispositivos clientes y falencias de conocimiento sobre seguridad de la información, fue necesario abordar diferentes aspectos, tales como capacitar y concientizar a los colaboradores del uso de los recursos tecnológicos, los riesgos cibernéticos a los que se enfrentan cada día, instalar actualizaciones críticas en los diferentes equipos de la red, analizar y documentar el esquema del plan de copias de seguridad de la empresa y afinar aspectos de seguridad a los servidores que podrían llegar a verse afectados por un ataque tipo Ransomware.

Tips de Seguridad

Como parte del trabajo de concientización y capacitación de los empleados de "Servicios TI", se crearon algunos tips o consejos de seguridad básicos y se compartieron vía correo institucional, con el fin de que las personas que tienen muy pocas bases sobre las nuevas amenazas de ciberseguridad, hagan uso de las buenas prácticas o recomendaciones para protegerse frente al robo de información empresarial y/o personal. Estos tips de seguridad, se han tomado como base del fabricante de productos de cberseguridad "ESET", pero se han plasmado gráficamente para que el personal que no tenga mucho conocimiento técnico, pueda entender los conceptos intuitivamente.

Para la creación de estos tips de seguridad, se utilizó la herramienta de código abierto "GIMP" y los vectores fueron extraídos del sitio www.freepik.es, la cual contiene una gran base de datos con imágenes de libre uso.

En el primer tip de seguridad compartido a los colaboradores, se brindan siete (7), consejos de seguridad en general sobre ciberseguridad. Dentro de estos se encuentran los siguientes:

- No ignorar avisos del navegador sobre certificados: Estos avisos informan cuando un sitio utiliza un certificado SSL no verificado, lo cual puede ser una técnica de ataque, para descifrar todo el tráfico que pase por una red.
- Mantener aplicaciones y Antivirus Actualizados: Debido a que nacen nuevas amenazas de seguridad constantemente, los fabricantes de Antivirus realizan publicaciones de bases de datos a diario.
- No confiar en Wifi's Publicas: Un atacante, puede capturar todo el tráfico que viaje por esta.
- No dejar sesión abierta en el equipo: Una persona malintencionada podría robar información confidencial.
- Usar contraseñas seguras: Menos dificil de romper con técnicas de ataques tales como fuerza bruta o ataques por diccionario.
- No enviar información confidencial vía correo: Puede ser interceptada o caer en manos peligrosas.
- No abrir ni instalar aplicaciones de origen no verificado: Muchas de las aplicaciones o programas instalados de páginas o tiendas no oficiales, suelen contener software malicioso.

Gráfico 44. Tip de seduridad informática, para colaboradores de Servicios TI

En el segundo Tip de seguridad que se envió por medio del correo institucional al personal de "Servicios TI", se brindan ocho (8) consejos para mantenerse a salvo de infecciones y robo de información por amenazas tipo Ransomware. Estos consejos, fueron basados en la información que tiene a disposición la empresa de seguridad Netwrix (2019), donde explican detalladamente las mejores prácticas para prevenir infecciones por Ransomware.

Gráfico 45. Tip para evitar Ransomware, para colaboradores de Servicios TI

A continuación, se explican cada uno de los consejos y su importancia para prevenir infecciones por Ransomware:

Tip #1: Copias de Seguridad: Es necesario tener Backup de la información crítica ya sea personal o laboral. Es recomendable almacenar esta información en sitios alternos

tales como plataformas Cloud y almacenamientos externos tales como discos duros, cintas, USB's, entre otros.

Tip #2: Sea precavido al abrir correos: Analizar todos los campos de un nuevo correo. Se debe verificar la autenticidad remitente, del dominio desde donde se recibe, el asunto, la ortografía y validar que los enlaces no apunten a sitios extraños.

Tip #3: Mantenga actualizado todo su software: Por motivos de falencias de seguridad descubiertas en diferentes aplicativos, la mayoría de las fabricantes, publican actualizaciones de seguridad constantemente. Es de vital importancia aplicar estas actualizaciones de seguridad.

Tip #4: Manténgase al tanto de noticias de TI: Leer noticias en sitios que hablen sobre seguridad de la información, puesto que explican detalladamente al momento de presentarse nuevas amenazas, el modo en que estas trabajan y las mejores prácticas para prevenir un ataque de estas.

Tip #5: Utilice y actualice su Antivirus: Es necesario tener instalado y actualizado un software Antivirus, que ayude a identificar y remediar amenazas de seguridad de la información.

Tip #6: Bloquear remitentes desconocidos: No abrir enlaces ni archivos adjuntos de remitentes desconocidos, por el contrario, es recomendable reportar como Spam y bloquear este tipo de correos.

Tip #7: Evite las conexiones a Wifi's Públicas: Es importante evitar utilizar este tipo de conexiones o de abrir sitios bancarios, aplicativos que requieran inicio de sesión o abrir documentos importantes, cuando se encuentre conectado a este tipo de redes.

Tip #8: Bloquear publicidad en su computador: Utilizar programas para bloquear contenido publicitario en los navegadores WEB, debido a que estos contienen malware que pueden afectar información de los usuarios.

Backup de la información

Tenienido en cuenta las recomendaciones sobre la protección de la información por parte de la empresa (Sonicwall Inc., 2017), la cual habla acerca de que, si una empresa tiene una buena estrategia de copias de seguridad, en caso de una infección por Ransomware, no habría necesidad de pagar por el rescate de la información. Con base en lo anterior, fue necesario analizar el esquema de respaldo de la información de le empresa "Servicios TI", con el fin de verificar si realmente se está realizando una gestión de Backups efectiva.

En la actualidad, Servicios TI cuenta con un total de 22 servidores productivos en ambientes virtualizados, a los cuales se les realiza copia de seguridad diaria en las horas de la madrugada con la herremienta Veeam Availability Suite, en sistemas de almacenamiento ubicados en la sede principal de la compañía. Posterior a la ejecución de las copias de seguridad, la herramienta Veeam realiza una ráplica de los backups hacia un centro de datos alterno ubicado a 30 Kms de las instalaciones de Servicios TI (por motivos de seguridad no es posible brindar ni la ubicación, ni la empresa con la cual se tiene contratado el servicio de datacenter de respaldo). Finalmente, se realiza una nueva réplica de la información desde el centro de datos alterno, hacia un ambiente de nube pública contratado

con la empresa Microsoft Azure, esta última copia de la información se realiza por medio de una conexión cifrada a través de Internet por un protocolo llamado VPN Ipsec.

Con el objetivo de tener visibilidad sobre el esquema de esta conexión, se ha creado un diagrama de la topología de la gestión de respaldos de información. Por motivos de privacida, en la topología que se presenta en este documento no es posible mencionar direcciones IP, direcciones de los centros de datos, versiones de los aplicativos de respaldo, entre otros datos.

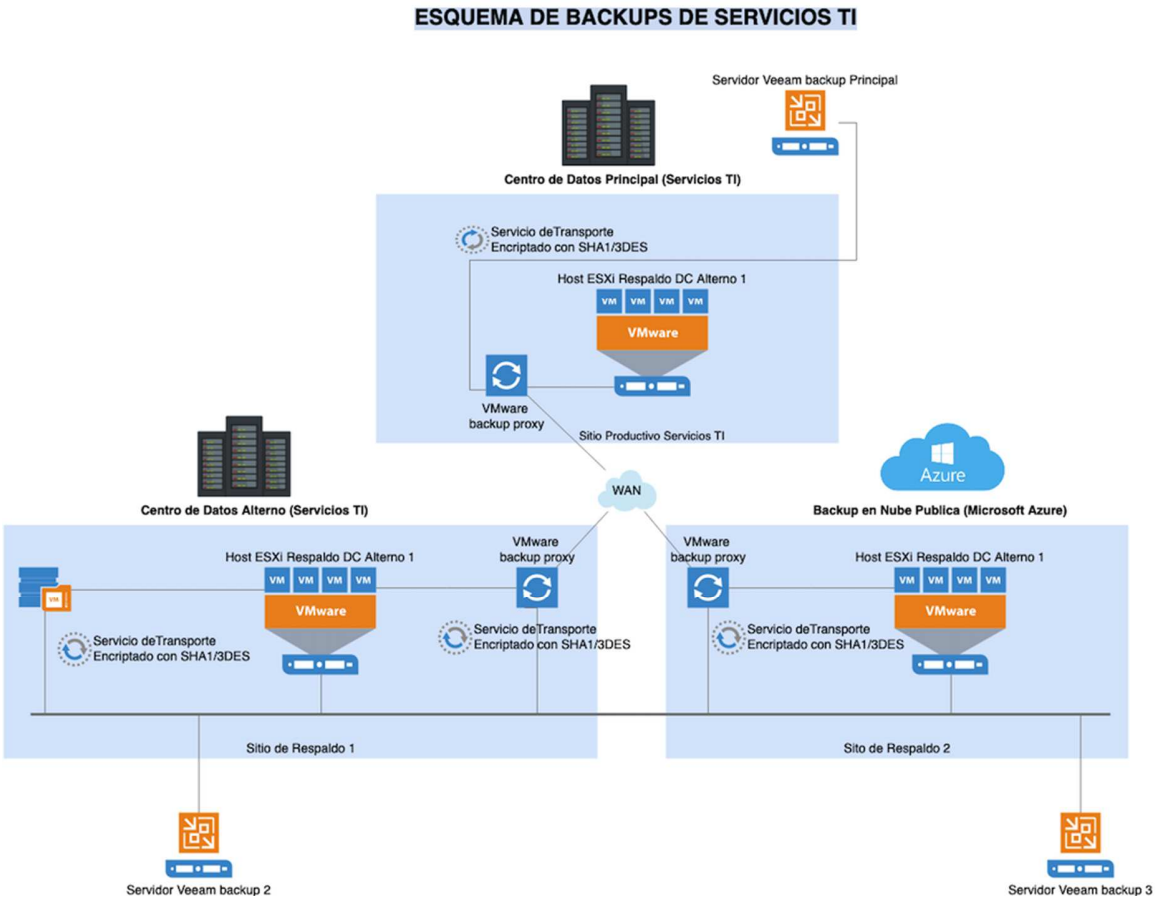


Gráfico 46. Estructura de Backup de Servicios TI

Aplicación de Actualizaciones

Con base en el análisis de vulnerabilidades realizado, fue necesario remediar las vulnerabilidades asociadas a Ransomware (MS17-010: Security Update for Microsoft Windows SMB Server- 4013389), las cuales se encontraron en dos (2) servidores de Servicios TI, los cuales fueron CAOS y HEFESTOS.

Para verificar si los servidores tienen o no instalado el parche de seguridad para remediar los ataques de Ransomware, la empresa ESET, pone a disposición una herramienta gratuita, la cual verifica si un equipo con sistema operativo Windows, tiene instalada la actualización (MS17-010). El enlace para descargar dicha herramienta y el manual de uso es el siguiente:

https://www.welivesecurity.com/la-es/2017/05/16/check-eternalblue-pc-parcheada-wannacry/

Análisis previo e instalación en los servidores "CAOS y HEFESTOS".

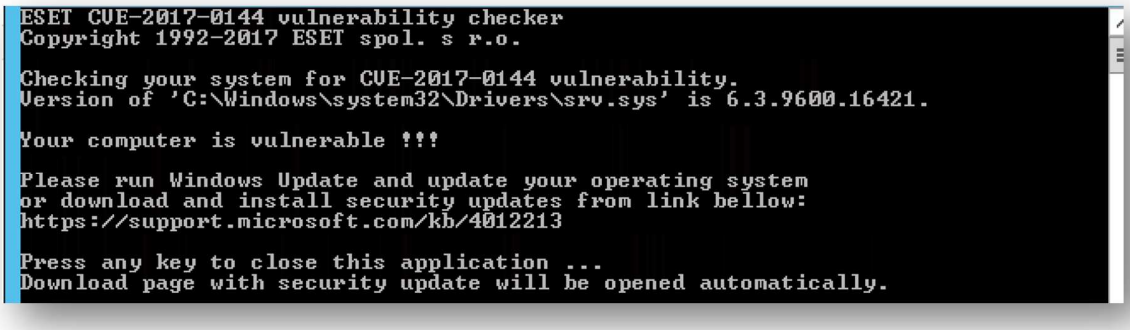


Gráfico 47. Análisis de parche sobre Ransomware

Como se puede observar en la imagen anterior, aparece el mensaje “Your computer is vulnerable”, lo cual indica que el servidor aún no tiene instalado el parche de seguridad para remediar la vulnerabilidad asociada a Ransomware. Para instalar la actualización, es necesario descargar de la página oficial de Microsoft, el parche adecuado a la versión del sistea operativo instalado en este caso es Windows Server 2012 R2 Standard. Al descargar el archivo lo podrá visualizar de la siguiente manera:

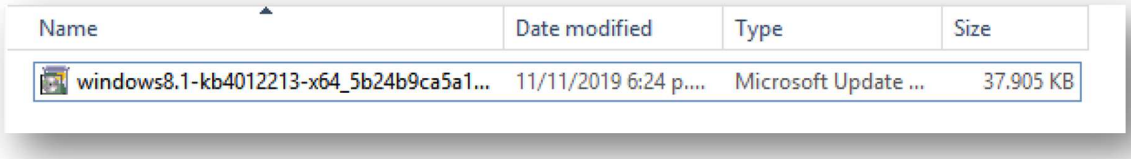


Gráfico 48. Ícono del parche MS17-010

Para instalar el parche, es necesario ejecutar con privilegios de administrador el aplicativo utilizando el comando “DSIM.exe /online /ad-package Ruta del paquete”, inmediatamente se desplegará una ventana de linea de comandos indicando el progreso de la instalación, versión de la actualización y la notificación de finalización.

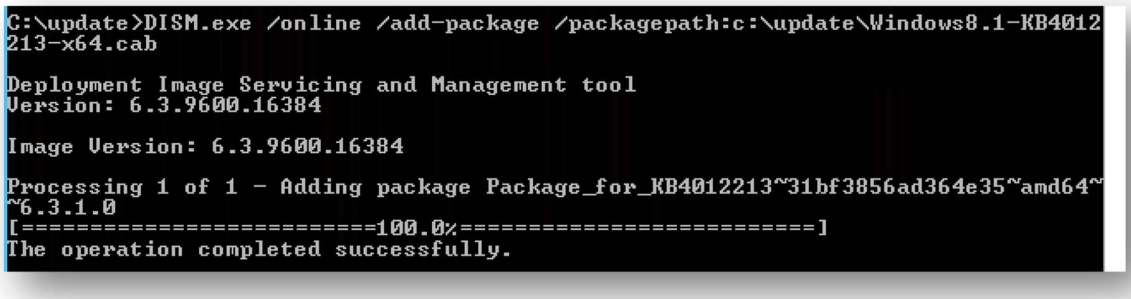


Gráfico 49. Progreso de la instalación del parche MS17-010

Posteriormente, se debe forzar en el equipo la búsqueda de actualizaciones automáticas, lo cual terminará la instalación del parche agregado en el paso anterior.

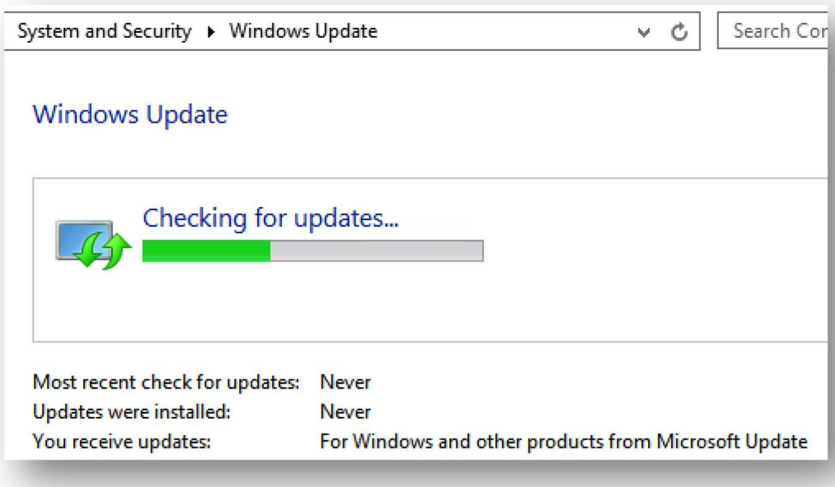


Gráfico 50. Actualización del Servidor

Cuando el aplicativo de actualizaciones de Windows termine de buscar las actualizaciones, inmediatamente empezará la instalación del parche “KB4012213”, tal como se observa a continuación:

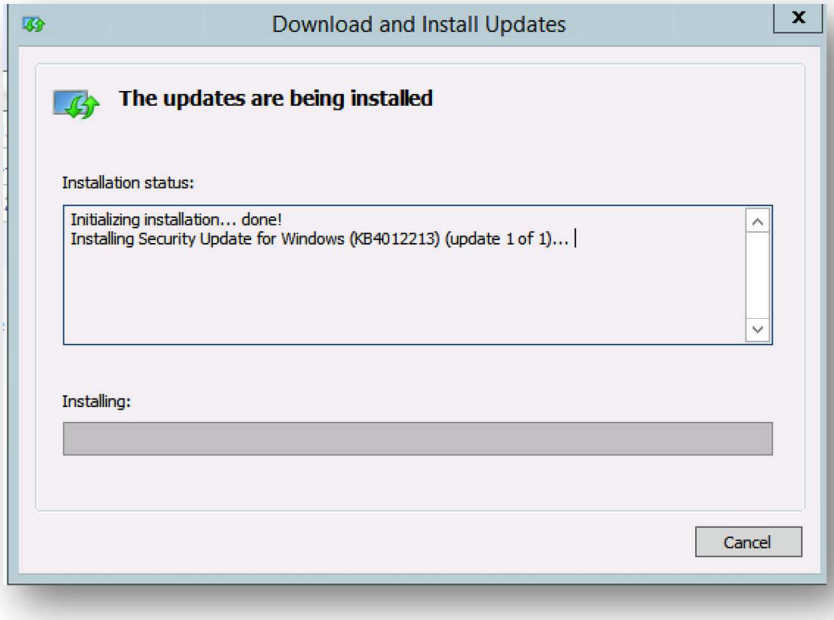


Gráfico 51. Finalización de la instalación del servidor

Al finalizar la instalación, aparecerá una notificación informando que el equipo ya cuenta con la actualización que mitiga la posibilidad de infección por Ransomware de los servidores de Servicios TI, tal como se objerva a continuación:

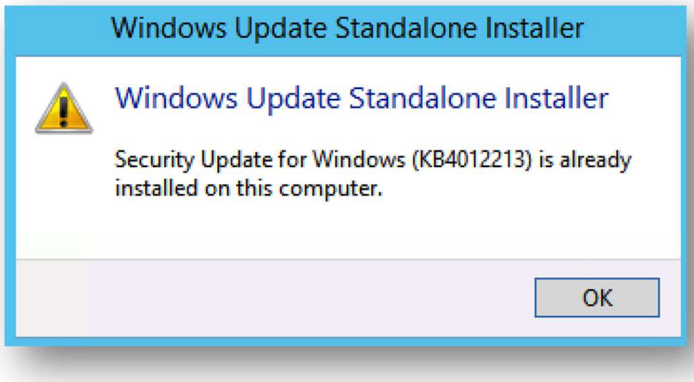


Gráfico 52. Notificación informando que el parche fue correctamente aplicado

Finalmente, es necesario verificar si el parche fue aplicado correctamente, para esto se recomienda utilizar la herramienta de verificación de ESET, la cual arroja el resultado "Your computer is Safe", indicando que la actualización fue aplicada correctamente y el servidor se encuentra protegido frente a un ataque de Ransomware.

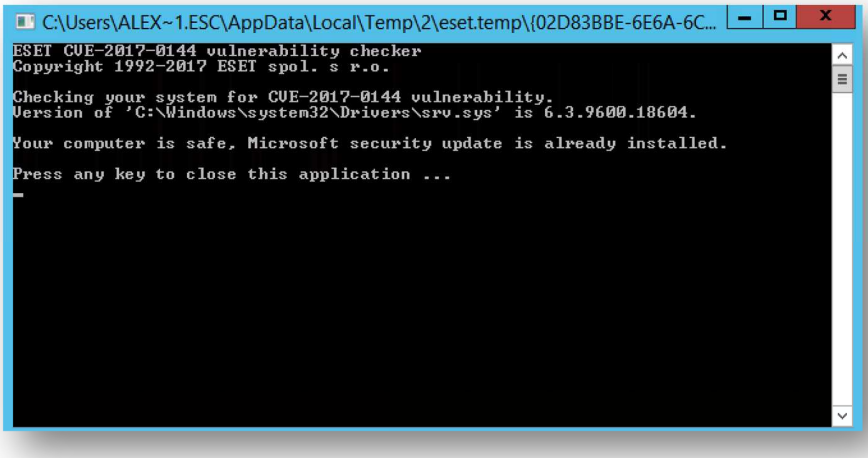


Gráfico 53. Verificación por linea de comandos de la instalación del parche

Con el procedimeinto anterior, se mitiga la vulnerabilidad denominada por Microsoft como "MS17-010", la cual permite la propagación de Ransomware vía el protocolo SMB (Protocolo para compartir archivos en red). No obstante, es necesario revisar constantemente que las actualizaciones del sistema operativo se estén aplicando adecuadamente, con el fin de que los servidores y equipos clientes, no se encuentren expuestos a nuevos ataques y nuevas técnicas de intrusión.

Afinamiento adicional

Adicional a la instalación de las actualizaciones de seguridad y siguiendo el manual de buenas prácticas del Instituto Nacional de Ciberseguridad de España (INCIBE), es necesario utilizar los criterios de "Mínimos privilegios", para los usuarios con el fin de proteger la gestión de accesos dentro de la red, así como también desactivar la versión 1 del protocolo SMB (Compartir archivos en red), debido a que este cuenta con múltiples falencias de seguridad, las cuales son aprovechadas por el Ransomware para infectar y propagarse dentro de una red.

Desactivar SMB v1.

Se desactiva el protocolo SMB v1, en todos los 18 servidores Windows de la empresa Servicios TI, con el fin de que si se requiere compartir archivos en red, se haga uso del protocolo en su versión 2 y 3 a los cuales les fueron aplicadas múltiples mejoras con respecto a la seguridad. Adicionalmente, es de vital importancia desactivar este protocolo debido a que las nuevas variantes de Ransomware siguen utilizando el mismo mecanismo para infectar equipos de una red.

El procedimiento para desactivar el protocolo en cada uno de los servidores, fue ingresar al administrador de roles y características, buscar el apartado de carácterísticas, seguidamente buscar y deshabilitar la opción "SMB v1/ CIFS File Sharing Support", tal como se muestra a continuación:

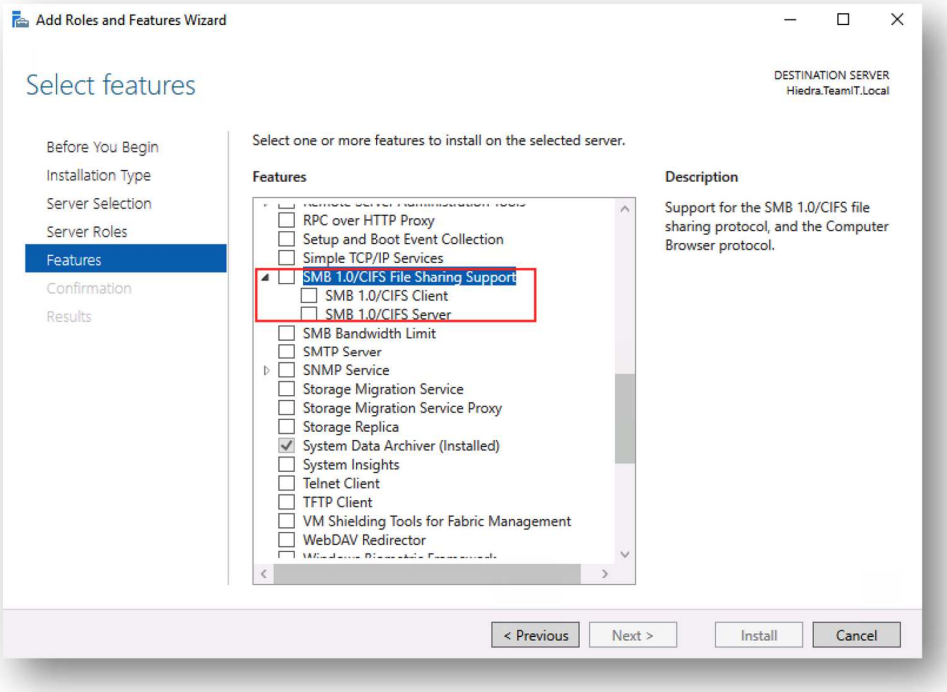


Gráfico 54. Evidencia de desactivación de SMB versión 1

Habilitar mínimos privilegios

El concepto de mínimos privilegios consiste básicamente en minimizar el impacto de cualquier fallo, accidente o vulnerabilidad del sistema, reduciendo los privilegios de la cuenta de usuarios al mínimo necesario para el desempeño de sus tareas autorizadas. Dado que este principio está directamente relacionado con los distintos perfiles creados dentro del sistema operativo, los expertos recomiendan disponer de al menos dos cuentas básicas. La primera de ellas tendrá privilegios de administrador para poder gestionar el sistema y la instalación del software, con la precaución de renombrar la cuenta bajo un seudónimo para

no revelar la identidad de esta. La segunda tendrá privilegios limitados con el acceso a la manipulación de la configuración del equipo y su software totalmente restringido.

Como parte final del afinamiento en Servicios TI, se aplicó en veinticinco (25) equipos del área administrativa, una configuración con el fin de que los usuarios no puedan instalar ningún tipo de aplicativo ni realizar modificaciones al sistema, sin tener las credenciales del administrador del dominio de la compañía. La configuración de los privilegios se modificó ingresando a las propiedades avanzadas del sistema de cada uno de los equipos (Panel de Control), Se eligió la opción cuentas de usuario, seguido a esto se seleccionaron las cuentas de usuario final que se desean proteger y se les asigna como pertenencia el perfil de otros "usuarios". La configuración se puede observar a continuación:

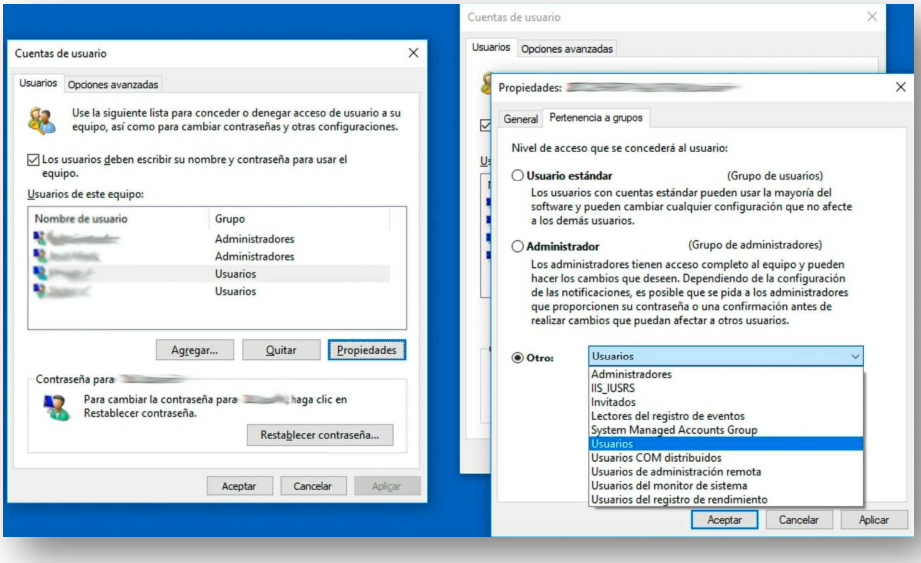


Gráfico 55. Evidencia de cambios en privilegios de usuarios

Finalmente, se intenta desde uno de los equipos a los cuales se les modificó el perfil de usuario, instalar un software gratuito e inmediatamente aparece en pantalla un recuadro para ingresar las credenciales de un usuario administrador, tal como se observa en la siguiente imagen:

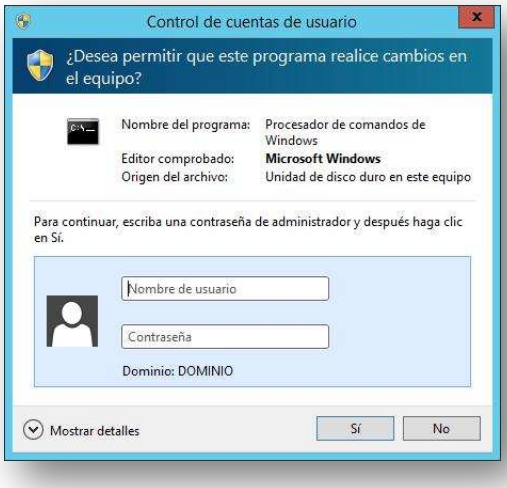


Gráfico 56. Solicitud de credenciales

Capítulo 6

Conclusiones y recomendaciones

- La realización del inventario y el análisis de impacto para el negocio de los principales servidores, servicios y plataformas, es de mucha utilidad para la compañía, puesto que brinda a Servicios TI una priorización de los recursos y puede conocer donde se presentan las principales falencias de seguridad.

Fue sumamente importante la ejecución del análisis de vulnerabilidades, debido a que se encontraron amenazas críticas, asociadas a posibles ataques de malware tipo Ransomware, en servidores críticos de la compañía. Además, se encontraron múltiples vulnerabilidades en servicios publicados en Internet, en los cuales los clientes de la empresa almacenan información confidencial.

La documentación detallada sobre las brechas de seguridad encontradas y la remediación a estas, fue de las actividades más importantes de este proyecto de grado, puesto que se solucionaron vulnerabilidades y se estará evitando una posible afectación a la confidencialidad e integridad de la información, así como de los servicios suministrados a los clientes internos y externos.

Con las remediaciones aplicadas, se han reducido considerablemente las probabilidades de presentar una infección en servidores y equipos de usuario final por una amenaza tipo Ransomware, lo cual brinda una mayor confianza por parte del personal interno, de proveedores y de clientes al ver que Servicios TI aplica buenas prácticas para tener a salvo información que pueda afectar la continuidad del negocio.

Adicionalmente, es recomendable establecer dentro de las políticas de seguridad de la información, una periodicidad para la ejecución de un análisis de vulnerabilidades de los recursos internos y de los servicios publicados en Internet.

Finalmente, se recomienda mantener actualizado en la medida de lo posible los diferentes sistemas operativos, firmware y demás plataformas de la compañía.

Resultados

1. Se realizó un análisis de madurez, para determinar el estado de los recursos, configuraciones, activos y aplicaciones, referente a temas de seguridad de la información. Con este insumo, se tendrá una ponderación relacionada a la seguridad de los datos sobre cada uno de los recursos críticos de la compañía por medio de un indicador, por medio del cual posiciona a la empresa en un rango de madurez, el cual posibilitará enfocarse a resolver estas debilidades y de este modo no comprometer información crítica para continuidad del negocio.

2. Se realizó un informe ejecutivo, sobre las amenazas encontradas en los diferentes recursos de la compañía, incluyendo Direcciones IP, Subdominios, nombre de la amenaza encontrada, el tipo de severidad, observaciones y enlaces a informes de expertos en seguridad de la información referentes a dichas muestras. También quedó en evidencia las debilidades con las que contaba previamente la empresa, las cuales pudieron ser aprovechadas por una amenaza de secuestro de información tipo "Ransomware".

3. Se ejecutaron las remediaciones, las cuales se basaron en informes y estudios de fabricantes de soluciones de seguridad informática, las cuales incluyeron actualizaciones de software o mejoras a nivel de desarrollo interno, realizar cambios sobre configuraciones débiles, desactivar protocolos utilizados por el

Ransomware en equipos Clientes y servidores e instalar parches relacionados a esta amenaza.

4. Se realizó un test de correo fraudulento tipo “Phishing”, por medio del cual se compartió un correo similar al de un proveedor de servicios, pero este contenía un enlace hacia un sitio que simulaba una infección por Ransomware. A partir de esta prueba, se determinaron que acciones llevar a cabo para concientizar a los usuarios finales.

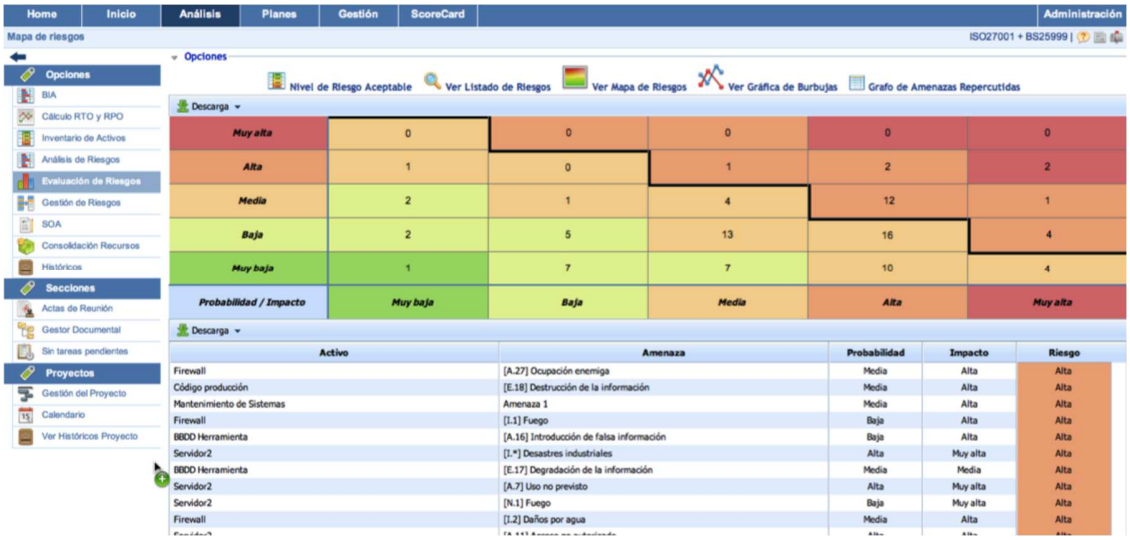
Finalmente, se crearon y compoartieron “Tips” o consejos por medio de la Intranet de la compañía, correo electrónico y diferentes canales de comunicación para los empleados, sobre el funcionamiento de un Ransomware, las consecuencias para el negocio y las mejores estrategias para protegerse de esta amenaza cibernética con el fin de concientizar al eslabón más débil en la cadena de la seguridad de la información que son los usuarios.

Listado de Anexos

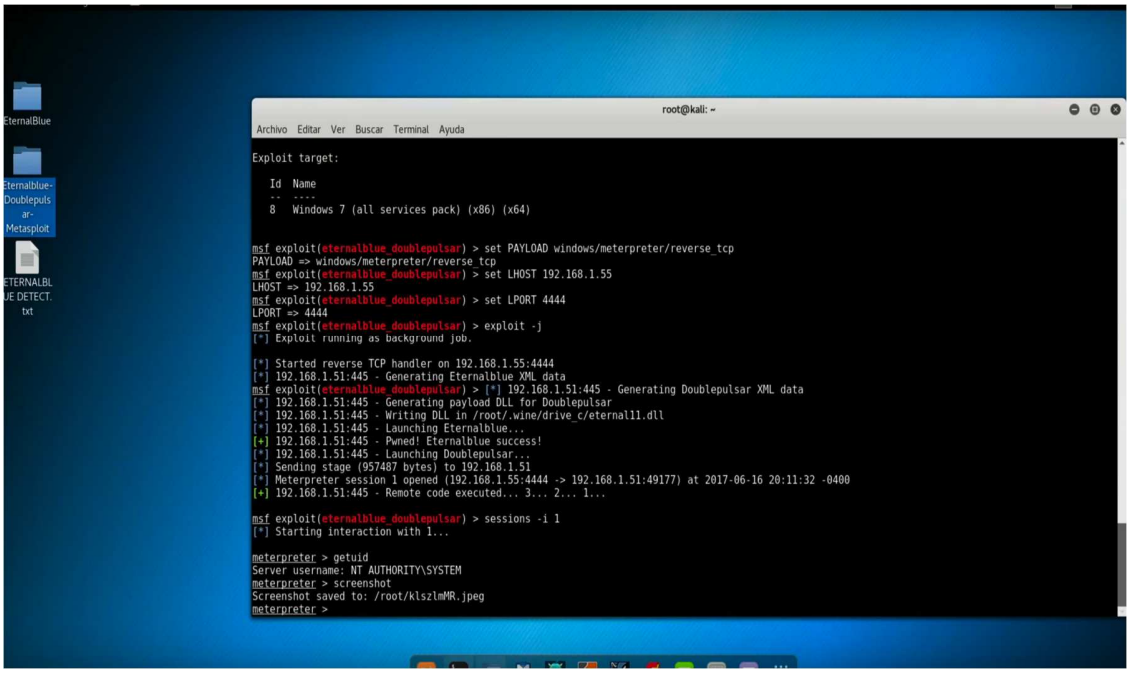
Anexo A. Plantilla del análisis de madurez

Peso General	Categoria	Criterio	Peso	Avance	Ponderación	Observaciones
16%	Visibilidad	Eventos en tiempo real	25,0%	70,0%	17,5%	Visibilidad perimetral y de equipos conectados direc
	Visibilidad	Analisis de aplicativos, servicios y protocolos de red por SNMP	25,0%	50,0%	12,5%	Herramienta de alertas tempranas y monitoreo
	Visibilidad	Monitoreo NOC o SOC (Nagios, Cacti, Zabbix)	25,0%	90,0%	22,5%	Se tiene configurada la herramienta Zabbix
	Visibilidad	Sistemas de Generación de Reportes	25,0%	20,0%	5,0%	Fortianalyzer y Syslog - Reportes completos FAZ
13%	Estandarización	ITIL, COBIT, Agile, Scrum - Gestión de Eventos	20,0%	20,0%	4,0%	No se tiene estructurado con base a un estándar la gestión de eventos y/o derroteros a seguir durante determinada situación de contingencia, instalación o modificación
	Estandarización	ITIL, COBIT, Agile, Scrum - Gestión de Disponibilidad	8,0%	20,0%	1,6%	No se tiene documentación referente a Plan de Recuperación ante desastres
	Estandarización	ITIL, COBIT, Agile, Scrum - Gestión de Incidentes y Requerimientos	20,0%	90,0%	18,0%	Se tiene implementada Mesa de Ayuda
	Estandarización	ITIL, COBIT, Agile, Scrum - Gestión de Capacidad	13,0%	15,0%	2,0%	No se tiene implementado un Capacity Planning
	Estandarización	ITIL, COBIT, Agile, Scrum - Gestión de Continuidad	13,0%	65,0%	8,5%	Se tienen configuradas réplicas de servidores hacia sitios alternos
	Estandarización	ITIL, COBIT, Agile, Scrum - Gestión de Configuración	13,0%	20,0%	2,6%	No se tiene un sistema automatizado para configurar equipos o plantillas para servidores y máquinas virtuales
	Estandarización	Modelo de operación	13,0%	40,0%	5,2%	Backups Manuales, Hardening sobre Firewall ppal apl
13%	Optimización (UTM)	Web Filter	20,0%	98,0%	19,6%	Perfiles aplicados a políticas de navegación
	Optimización (UTM)	AppControl	20,0%	98,0%	19,6%	Aplicación de APPControl a Wifi y LAN
	Optimización (UTM)	IPS/IDS	20,0%	95,0%	19,0%	Gestión de perfiles IPS
	Optimización (UTM)	DoS	20,0%	90,0%	18,0%	Gestión de perfiles DoS
	Optimización (UTM)	QoS	20,0%	40,0%	8,0%	Se tienen reglas de QoS muy básicas
25%	Gestion del riesgo	Analisis de Vulnerabilidades (Nessus, OpenVas, MetaSploit, Etc)	18,0%	70,0%	12,6%	Se realiza, pero no con constantemente
	Gestion del riesgo	Analisis de riesgo (Impacto)	18,0%	80,0%	14,4%	Pruebas DRP (Verificar)
	Gestion del riesgo	Web Aplication Firewall WAF	16,0%	0,0%	0,0%	NO hay WAF
	Gestion del riesgo	Afinación de perfiles y Firmas IPS	16,0%	60,0%	9,6%	Se han optimizado perfiles IPS y Firmas según servicio
	Gestion del riesgo	Aplicación de controles en servicios vulnerables	16,0%	80,0%	12,8%	Parchado parcial de ransomware, Crypto Miner, Petya, SamSam, Entre Otros.
	Gestion del riesgo	Protección a Distributed Deny of Service DDoS	16,0%	90,0%	14,4%	Hay avances con DoS Feature del Fortigate
20%	Gestion de red LAN y WL	Control de VLANs y Subnetting	18,0%	98,0%	17,6%	Falta documentación del subnetting
	Gestion de red LAN y WL	Inventario de activos y puntos de red	18,0%	50,0%	9,0%	Se tiene marcación de puntos de red, falta document
	Gestion de red LAN y WL	Gestión de direccionamiento público	12,0%	80,0%	9,6%	Se tiene control de las publicaciones, pero falta docu
	Gestion de red LAN y WL	DMZ y zonas seguras definidas	13,0%	40,0%	5,2%	Definir Subredes DMZ para publicación de servicios a
	Gestion de red LAN y WL	Estado de salud en red LAN y WLAN	15,0%	25,0%	3,8%	Se debe realizar un HealthCheck de las configuraciones y hardening de networking de la
	Gestion de red LAN y WL	Adecuaciones Fisicas	12,0%	98,0%	11,8%	Falta documentación sobre el cableado del Datacent
	Gestion de red LAN y WL	Control de acceso y perfiles de usuarios administradores	12,0%	50,0%	6,0%	Cambiar contraseñas y accesos periodicamente de Switches y Firewall
13%	Aseguramiento de Redes	Autenticación VPNs (LDAP)	20,0%	98,0%	19,6%	Existen algunos usuarios locales en la plataforma de L
	Aseguramiento de Redes	Autenticación Multifactor/Token	18,0%	0,0%	0,0%	No existe plataforma de autenticación multifactor
	Aseguramiento de Redes	Servicios AAA(Servicios de identidad de Red y Autenticación)	17,0%	20,0%	3,4%	Se tiene autenticación por AD. No existe Port Security en Switches, ni acceso a nevegación por
	Aseguramiento de Redes	Autenticación de Conexiones LAN y WLAN	19,0%	80,0%	15,2%	Autenticación de WLAN con NPS, FSSO para navegaci
	Aseguramiento de Redes	Certificado Digital	26,0%	0,0%	0,0%	No se tienen certificados SSL emitidos por una CA

Anexo B. Herramienta de AudiSec “GlobalSuite”, para la gestión de riesgos basados en Iso 27001



Anexo C. Laboratorio para “Explotar” vulnerabilidad MS17-010 EthernalBlue con MetaSploit Framework



Nota aclaratoria: *La información, datos y citas contenidas en el presente documento corresponden a fuentes bibliográficas y/o cibergráficas verídicas y susceptibles de confirmación por parte de Uniminuto Seccional Bello. De encontrarse copia, plagio o adulteración de cualquiera de las fuentes, el estudiante acepta su responsabilidad procesal en el hecho.*

En el documento no se menciona el nombre verdadero de la compañía en la cual se basó el trabajo, cuando se hace referencia, se nombra a la empresa "Servicios TI", el cual es un nombre creado por los estudiantes.

Lista de referencias

Aristizabal, E. S. (2019). Estrategias y prevención de riesgos cibernéticos. Obtenido de Digiware: http://www.digiware.net/?q=es/blog/estrategias-y-prevencion-de-riesgos-ciberneticos

Welivesecurity By ESET. (12 de 11 de 2014). La importancia de identificar, analizar y evaluar vulnerabilidades. Obtenido de welivesecurity: https://www.welivesecurity.com/la-es/2014/11/12/identificar-analizar-evaluar-vulnerabilidades/

Microsoft. (21 de 08 de 2017). Soporte Técnico de Microsoft. Obtenido de Cómo comprobar que MS17-010 está instalado: https://support.microsoft.com/es-co/help/4023262/how-to-verify-that-ms17-010-is-installed

Tenable Nessus. (10 de Mayo de 2019). Using Tenable.io to Reduce the Risk of Ransomware Infections. Obtenido de On-Demand Webinar: https://es-la.tenable.com/webinars/using-tenable-io-to-reduce-the-risk-of-ransomware-infections?tns_redirect=true

Congreso de Colombia. (2009). LEY NO 1273, de 2009. Recuperado mayo 27, 2018, de https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Alexander, A. (2013). Análisis y evaluación del riesgo de información: un caso en la Banca. Aplicación del ISO 27001:2005. Consultado el 12 de julio de 2015 en: http://www.iso27000.es/download/Evaluacion_Riesgo_iso27001.pdf

Aristizabal, E. S. (2019). *Estrategias y prevención de riesgos cibernéticos*. Obtenido de Digiware: http://www.digiware.net/?q=es/blog/estrategias-y-prevencion-de-riesgos-ciberneticos

Welivesecurity By ESET. (12 de 11 de 2014). *La importancia de identificar, analizar y evaluar vulnerabilidades*. Obtenido de welivesecurity: https://www.welivesecurity.com/la-es/2014/11/12/identificar-analizar-evaluar-vulnerabilidades/

Microsoft. (21 de 08 de 2017). *Soporte Técnico de Microsoft.* Obtenido de Cómo comprobar que MS17-010 está instalado: https://support.microsoft.com/es-co/help/4023262/how-to-verify-that-ms17-010-is-installed

Tenable Nessus. (10 de Mayo de 2019). *Using Tenable.io to Reduce the Risk of Ransomware Infections*. Obtenido de On-Demand Webinar: https://es-la.tenable.com/webinars/using-tenable-io-to-reduce-the-risk-of-ransomware-infections?tns_redirect=true

Tenable Nessus. (10 de mayo de 2019). Using Tenable.io to Reduce the Risk of Ransomware Infections. Obtenido de On-Demand Webinar: https://es-la.tenable.com/webinars/using-tenable-io-to-reduce-the-risk-of-ransomware-infections?tns_redirect=true

Kaspersky Lab. (18 de septiembre de 2017). Comunicados de prensa. Obtenido de Kaspersky Lab: Brasil, México y Colombia lideran incidentes de secuestros digitales en América Latina: https://latam.kaspersky.com/about/press-releases/2017_kaspersky-lab-incidents-of-digital-kidnappings-in-latin-america

Lysa Myers. “11 formas de protegerte del Ransomware, incluyendo Cryptolocker”. Revista digital welivesecurity en español. (2015). ESET Latinoamérica. Disponible en: https://www.welivesecurity.com/la-es/2015/07/08/11-formas-protegerte-del-ransomwarecryptolocker/

Netwrix Inc. (2019). "How to Prevent Ransomware Infections: Best Practices". Obtenido de Netwrix Inc. Visibility Academy. Disponible en: https://www.netwrix.com/prevent_ransomware_best_practice.html

Sonicwall Inc. (2017). “8 formas de proteger su red contra el ransomware”. Revista digital Sonicwall en español. (2017). Disponible en: https://sonicwall-web.s3-accelerate.amazonaws.com/sonicwall.com/media/pdfs/ebook/es_lr_snwl-ebook-8waysransomware-eu-imag-29271-d1.pdf