CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

PABLO HERNANDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2024

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

PABLO HERNANDEZ

Nombre

LUIS FERNANDO ZAMBRANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2024

CONTENIDO

RESUMEN

Este trabajo formula estrategias de contención y remediaciones aplicadas transformadas en capacidades técnicas en los equipos red team y blue team, durante el seminario especializado se realizaron diferentes actividades de identificación y remediación de vulnerabilidades, cada actividad concluye beneficios también abre posibilidades de conocer cómo actúan los ciberdelincuentes explotando vulnerabilidades en sistemas y redes. Teniendo claro los aspectos que se ejecutaron se deben entregar conclusiones que orienten a la organización a mostrar la necesidad de invertir en seguridad informática toda recomendación resaltara los beneficios de su implementación abarcando diferentes puntos débiles de una infraestructura.

Los ciberataques causan daños incalculables siendo la parte financiera una de las más afectadas, aquí se desencadenan daños a la reputación de marca, costos de litigio y multas regulatorias establecidas en códigos penales castigando con severidad la violación de los datos, la información confidencial se están convirtiendo rápidamente en la nueva normalidad obligando a los organismos legales a tomar medidas para proteger y mantener los sistemas en funcionamiento estas leyes pueden aplicarse generalmente en todo el país o solo a sectores específicos. Incluso si una empresa logra evitar dichas sanciones, seguirá incurriendo en gastos indirectos relacionados con las interrupciones operativas y el tiempo de inactividad causado por un ciberataque.

GLOSARIO

CIBERATAQUE: Intentos mal intencionados por robar, exponer y alterar información mediante el acceso no consensuado esto ocurre en una red informática comercial o personal.

CONFIDENCIALIDAD: Consiste en garantizar la privacidad y seguridad de los datos, y que la exposición de estos sea solo a personas autorizadas. Las herramientas de ayuda que puede encontrar una empresa para solidificar son los sistemas de encriptación y marcos de seguridad.

ECOSISTEMA DIGITAL: Es un conjunto dinámico y creciente de relaciones entre diferentes empresas con el objetivo de crear valor de forma conjunta para sus clientes mutuos. Al aprovechar los recursos compartidos entre las partes interesadas las organizaciones pueden aumentar la agilidad, reducir los costos y abrir nuevas oportunidades de ingresos.

INGENIERIA SOCIAL: Cualquier acto que influya en una persona para que realice una acción que puede o no ser lo mejor para sus intereses, estos métodos buscan manipular y jugar con las emociones de una víctima con el objetivo de que se revele información confidencial.

PHISHING: Se produce cuando los delincuentes utilizan técnicas para falsificar correos electrónicos, publicaciones en redes sociales o mensajes directos con el objetivo de incitarlo a hacer clic en un enlace incorrecto o descargar un archivo adjunto malicioso. Si por descuido o desconocimiento se hace clic puede entregar su información personal o corporativa a los ciberdelincuentes, también puede generar puertas traseras permitiendo la entrada a intrusos.

RED TEAM: Práctica de probar la seguridad de los sistemas de una organización emulando a un actor malicioso y pirateando sistemas o datos seguros, métodos que permite detectar falencias.

BLUE TEAM: Evalúan los entornos de seguridad organizacionales y defienden estos entornos de los equipos rojos. Las personas en este rol deben tener diferentes conocimientos y estos deben ser usados para una defesa de la entidad.

SANCIONES: Las sanciones son medidas económicas destinadas a presionar o castigar a los malos actores (ya sean individuos, grupos o países) que violan las normas internacionales o amenazan los intereses nacionales. Las sanciones en aspectos de ciberseguridad castigan a las entidades que sean víctimas de ciberataques ya que son los responsables de la confidencialidad de los datos.

VULNERABILIDAD: Debilidad que pueden aprovechar los ciberdelincuentes para obtener acceso no autorizado a un sistema informático. Después de explotar una vulnerabilidad, un ciberataque puede ejecutar código malicioso que busca beneficios monetarios individuales.

INTRODUCCIÓN

En el siguiente documento encontrara el reencuentro de prácticas y remediaciones utilizadas por los equipos rojos y azules. Dentro del desarrollo también se tiene en cuenta a los equipos morados que combina los mejores atributos de los equipos rojo y azul operando en un entorno colaborativo. Identifican vulnerabilidades dentro de la infraestructura de seguridad de una organización, evalúan las medidas defensivas existentes y desarrollan planes integrales para abordar las debilidades.

El correcto funcionamiento de toda organización gira entorno a su información ya que esto hace parte de la credibilidad, reputación y confianza que brinda a sus afiliados, los ataques cibernéticos han tenido un aumento considerable por esto es importante que en la época actual se custodie y se responda por la confidencialidad de cada uno de los socios. Pero lo que se debe hacer es fortalecer la infraestructura y aumentar el conocimiento interno de la seguridad, teniendo así una visión clara de cómo se está y como se debe estar en defensa cibernética, teniendo en cuenta todo el camino y actividad recorrida a lo largo del seminario se detallan conclusiones aplicables al entorno de TI brindando un papel importante a los equipos azules, rojos y morados quienes concentran un presente y destino en los pilares de seguridad.

OBJETIVOS

1.1 OBJETIVOS GENERAL

Emplear las mejores prácticas y métodos de remediación frente a un ataque cibernético mejorando de esta manera aspectos y tácticas de ciberseguridad en entornos T.I

1.2 OBJETIVOS ESPECÍFICOS

- Demostrar como los equipos azules y rojos identifican y generan ataques cibernéticos en tiempo real, mencionando prácticas a nivel performance y administración que buscando reducir la exposición de ciberdelincuentes.

- Evaluar características y aportes de los equipos azules y rojos evaluando las vulnerabilidades de la red mostrando la importancia de probar los sistemas de seguridad de su propia organización después de implementar un nuevo software o programa de seguridad en la combinación.

- Convencer al equipo de alta gerencia por medio de aspectos importantes los beneficios de invertir en seguridad informática contribuyendo al éxito general de la organización y de esta manera obtener una ventaja competitiva de infraestructura y políticas de ciberseguridad solidas.

LISTA DE GRAFICAS

DESARROLLO DEL TRABAJO

1.3 DE QUÉ MANERA PUEDEN APORTAR EN EL CAMPO DE LA CIBERSEGURIDAD LA INTEGRACIÓN DE EQUIPOS BLUE TEAM, RED TEAM Y PURPLE TEAM AL MISMO TIEMPO DENTRO DE UNA ORGANIZACIÓN.

Con el paso de **red team** se puede medir las debilidades en la política desplegada en la empresa, procedimientos y respuesta.
El impacto de las pruebas pinta un panorama mucho más amplio que ayudará la organización a priorizar y planificar sus futuras iniciativas de seguridad.

El equipo rojo juega un papel clave en la igualdad del campo de juego entre el atacante y el defensor. Permite a los defensores deshacerse de su postura reactiva, asumir la mentalidad del atacante y adoptar un enfoque agresivo para eliminar las vulnerabilidades de seguridad.
Si bien algunas organizaciones pueden confiar en la "seguridad por oscuridad" o sentir que su tamaño más pequeño las convierte en un objetivo poco probable, la verdad es que ninguna empresa está a salvo.[1]
Los atacantes a menudo eligen empresas más pequeñas porque el nivel de defensa es más bajo o porque desean utilizar la red de esa empresa como escenario para un ataque separado a una empresa más grande más adelante en la cadena de suministro. La formación de equipos rojos también es lo suficientemente flexible como para centrarse en las amenazas que son específicas del tamaño o la industria de una empresa, lo que la hace adaptable a casi cualquier organización.

Practicar es clave cuando se aprende a detectar y responder a una violación. Es importante medir el progreso para ver realmente el crecimiento. Es difícil determinar

[1] ORDOÑEZ, Wilinton. Red Team, Blue Team y Purple team: Guía completa sobre los equipos en Ciberseguridad. Ciberseguridad, tecnología e innovación | GroupHacking [página web]. (23, julio, 2023). [Consultado el 2, abril, 2024]. Disponible en Internet: <https://www.grouphacking.com/ciberseguridad/hacking-etico/red-team-blue-team-y-purple-team-guia-completa-sobre-los-equipos-en-ciberseguridad/>.

la hora exacta en que ocurre una violación, lo que hace que sea aún más difícil responder adecuadamente. Es por eso que los ejercicios del equipo rojo son tan importantes. Durante un ejercicio de equipo rojo, el equipo capturará el tiempo de cada acción para medir efectivamente la detección y respuesta de las personas, el proceso y la tecnología. Las organizaciones tienen proveedores de consultoría sobre retenedores para responder a ataques como realizar análisis forenses digitales y respuesta a incidentes (DFIR). Al probar y medir las personas, los procesos y la tecnología, las organizaciones estarán equipadas para asignar un presupuesto preciso a estos proveedores de servicios. Esto les permitirá probar qué tan rápido pueden sus proveedores de servicios a bordo para ayudar en un ataque real.

Defender (**blue team**) es más complejo que atacar y es más crucial, proteger la infraestructura TI es el objetivo trazado estar alerta las 24 horas del día, los 7 días de la semana, los 365 días del año para proteger su infraestructura. Como atacante, puede elegir una hora/fecha específica para lanzar un ataque o ejecutar aburridos ataques de fuerza bruta en muchos objetivos potenciales. Debe proteger todos los eslabones débiles de su infraestructura (fotocopiadora, impresora, sistema de asistencia, sistema de vigilancia o terminal utilizado por su recepcionista), mientras que los atacantes pueden seleccionar cualquier sistema conectado a su infraestructura. Como defensor, deber estar preparado por el equipo rojo que ayuda en el trabajo creando escenarios de ataque para poner a prueba las capacidades de blue team capacidades.

Traer investigadores nuevos y experimentados es costoso y complicado. Las organizaciones deberían esforzarse por promover y alentar a los analistas de entrada a aprender y experimentar con nuevas habilidades y tecnologías. Si bien los gerentes de SOC pueden temer que esto pueda interferir con las misiones diarias de los analistas experimentados o provocar que las personas abandonen la empresa, paradójicamente, alentará a los analistas a quedarse y participar más

activamente en la maduración de la seguridad de la organización casi sin costo adicional. De conseguir esta madurez aumenta la resiliencia cibernética de la empresa y proporciona medidas cuantificadas de la eficacia de su equipo azul a lo largo del tiempo.[2]

Mientras que el equipo rojo se preocupa por identificar vulnerabilidades, el equipo azul es responsable de brindar protección continua de por vida, por lo que la unión de ambos equipos puede mejorar la seguridad general.

La mayor ventaja es que se pide a dos equipos con diferentes conjuntos de habilidades y enfoques que evalúen los sistemas y las prácticas de seguridad de la organización. El resultado seguramente será un buen augurio para el futuro de la organización, ya que puede tapar todos los posibles puntos de entrada para los ataques cibernéticos.

El enfoque del **equipo morado** combina los mejores atributos de los equipos rojo y azul operando en un entorno colaborativo.

- Simulando ataques como los equipos rojos.
- Defenderse de esos ataques como equipos azules.

Identifican vulnerabilidades dentro de la infraestructura de seguridad de una organización, evalúan las medidas defensivas existentes y desarrollan planes integrales para abordar las debilidades. Este enfoque ayuda a las organizaciones a estar un paso por delante de posibles adversarios. Desde pruebas de penetración y evaluaciones de vulnerabilidad hasta simulaciones de respuesta a incidentes, los

[2] KEEPCODING. ¿Qué es Purple Team en ciberseguridad? KeepCoding Bootcamps [página web]. (21, julio, 2023). [Consultado el 3, abril, 2024]. Disponible en Internet: <https://keepcoding.io/blog/que-es-purple-team-en-ciberseguridad/>.

equipos morados aprovechan las diversas habilidades de los expertos ofensivos y defensivos para evaluar la efectividad de los controles de seguridad.

Los equipos morados dependen enteramente del intercambio de información entre los equipos rojos y azules. A través de sesiones de formación y talleres, potencian las habilidades de los miembros del equipo, equipándolos con las últimas técnicas y estrategias.

La respuesta a incidentes es un enfoque para manejar las violaciones de seguridad. El objetivo de la respuesta a incidentes es identificar el alcance de los eventos, contener el daño y mitigar o erradicar la causa raíz del incidente. Un incidente representa un cambio en la postura de seguridad que potencialmente infringe la ley, la política o un acto inaceptable que afecta a los activos de información, como redes, computadoras o teléfonos inteligentes, que pueden o no ser reportables materialmente.

1.4 PLANTEE POLÍTICAS DE SEGURIDAD Y RECOMENDACIONES PARA MEJORAR LOS ASPECTOS DE CIBERSEGURIDAD EN CUALQUIER ORGANIZACIÓN EN SUS ENTORNOS T.I.

Recomendable aplicar CIS “Center For Internet Security” La guía se basa en aportes de una amplia gama de expertos, lo que garantiza relevancia y practicidad. También se ajustan periódicamente para seguir el ritmo de la evolución de las ciberamenazas. Ofrecen un enfoque pragmático de la seguridad que no sobrecarga demasiado el rendimiento del sistema ni la productividad del usuario. Al seguir los puntos de referencia CIS, las organizaciones pueden mantener un alto nivel de seguridad sin comprometer la eficiencia de sus operaciones. Los puntos de referencia CIS representan las mejores prácticas de seguridad. Incluyen asesoramiento personalizado para diferentes plataformas, desde sistemas operativos hasta servicios en la nube.

CIS organización sin fines de lucro que se dedica a mejorar la seguridad cibernética a nivel global identificar, desarrollar y promover mejores prácticas de seguridad cibernética en su material encuentra mejores prácticas y tutoriales, este programa proporciona a las organizaciones una forma de mostrar a los clientes y socios postura de ciberseguridad seguras y confiables. [3]

Son cuatro módulos y a continuación se describe el contenido de cada sesión:

CIS CONTROLS:

Los controles CIS se alinean con diversas regulaciones de la industria, lo que brinda un camino hacia el cumplimiento de estándares como PCI DSS, HIPAA, GDPR, CMMC y más. De hecho, varias entidades gubernamentales reconocen los Controles CIS como punto de referencia para demostrar un nivel razonable de seguridad.

En la descripción general encontrara un video de un minuto que explica brevemente Pestaña características, donde se reúne el concepto de los 18 controles en grupos de Implementación (IG), que son categorías autoevaluadas que identifican un subconjunto específico de los Controles CIS

IG1: Está dirigido a pequeñas y medianas empresas con recursos limitados de TI y ciberseguridad, centrándose en salvaguardas que sean fáciles de implementar y diseñadas para contrarrestar ataques generales no dirigidos.

[3] IBM. ¿Qué son los puntos de referencia de CIS? | IBM. IBM in Deutschland, Österreich und der Schweiz [página web]. (1, junio, 2024). [Consultado el 28, marzo, 2024]. Disponible en Internet: <https://www.ibm.com/es-es/topics/cis-benchmarks>.

IG2: Se basa en IG1 al agregar salvaguardas para organizaciones con infraestructuras de TI más complejas y datos más confidenciales, abordando una mayor complejidad operativa y requisitos de cumplimiento normativo.

IG3: Incluye todas las salvaguardas de IG1 e IG2. Este IG está dirigido a organizaciones con experiencia especializada en ciberseguridad que manejan información sensible o funciones bajo una estricta supervisión regulatoria y de cumplimiento.

CIS Benchmarks List

Son recomendaciones de configuración prescriptivas para más de 25 familias de productos de proveedores.
Aquí encuentra la forma de reforzar sus sistemas operativos y como primer paso debe seleccionar el dispositivo de red, proveedor de nube o sistema operativo.
Paso dos corresponde a una subcategoría para la tecnología que utilice en su organización.
Una vez identificada la necesidad puede descargar los recursos disponibles, se recomienda descargar la versión actualizada.

Se tienen pasos opcionales donde será usted quien los seleccione de acuerdo a su necesidad de mejoramiento en los sistemas operativo.

CIS SecureSuite

Ofrece una variedad de recursos diseñados para ayudarle a proteger sus sistemas y datos. Incluye beneficios, herramientas y recursos que pueden ayudarle a implementar medidas de seguridad adecuadas y controlar la gobernanza utilizando nuestras mejores prácticas de seguridad basadas en consenso.

MS-ISAC

También viene funcionalidad Panel de control, que le ayuda a realizar un seguimiento de su cumplimiento durante un período de tiempo reciente para que pueda medir su progreso y planificar el futuro. Esto garantiza que no solo haya implementado, sino que también haya seguido sus medidas de seguridad. Como herramienta de gobernanza, esto permite transparencia, precisión y responsabilidad en su gestión de seguridad.

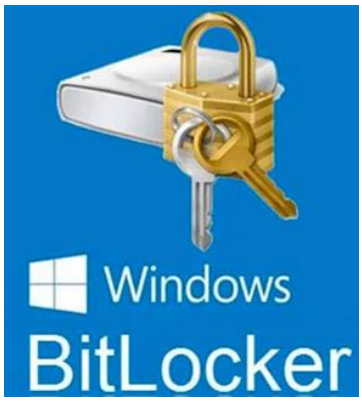
Este módulo explica cómo se benefician los miembros quienes tendrán acceso a una comunidad que lo ayudará a mantenerse actualizado sobre las amenazas cibernéticas que enfrenta su industria.[4]

» Otra alternativa de solución es usar Bitlocker, característica de ciertas versiones de Windows que cifra el contenido del disco duro. Sin la clave de descifrado correcta, es prácticamente imposible descifrar esta protección. Entonces, incluso si alguien abriera físicamente su PC, sacara su disco interno y lo conectara a otra computadora, no podría leer los datos sin esa clave. [5]

[4] BUGCROWD. CIS Controls Framework (Center for Internet Security) | Bugcrowd. Bugcrowd [página web]. (16, agosto, 2022). [Consultado el 28, marzo, 2024]. Disponible en Internet: <https://www.bugcrowd.com/glossary/cis-controls-framework-center-for-internet-security/>.

[5] GIL, Marc Bolufer. Análisis completo de las ventajas y desventajas de Windows 10 Pro: ¿Vale la pena? - Ventajas y desventajas top. Ventajas y desventajas top [página web]. (2, noviembre, 2023). [Consultado el 29, marzo, 2024]. Disponible en Internet: <https://ventajasydesventajastop.com/windows-10-pro-ventajas-y-desventajas/>.

Ilustración 1_Activación de BitLocker



Fuente: hungerford

» Una forma en que las organizaciones pueden evaluar sus capacidades de seguridad es organizar un ejercicio de equipo rojo/equipo azul. Estos dos equipos de profesionales se enfrentan para poner a prueba una infraestructura de seguridad en una simulación destinada a imitar un ataque real. Adoptar un enfoque de equipo rojo versus equipo azul para la ciberseguridad puede tener varios beneficios, permitiendo a los equipos de seguridad:

- Encuentra vulnerabilidades
- Fortalecer la seguridad de la red
- Desarrollar experiencia en la detección y contención de ataques.
- Desarrollar planes y procedimientos de respuesta.
- Crear competencia y cooperación sanas
- Crear conciencia sobre la seguridad entre el resto del personal

» Aplicar autenticación de dos pasos (MFA) confirmando la identidad de usuario que intenta el inicio de sesión, es decir, contraseña regular más un código

de una sola vez enviado a un teléfono inteligente. El acceso de los usuarios solo se permite tras la confirmación exitosa de ambos factores.[6]

Se requerirá MFA para acceder a las aplicaciones de Office 365, incluido el correo electrónico de Outlook, OneDrive, Skype for Business, desde fuera de la sede principal de la organización. Agregar una capa adicional de verificación de identidad con MFA ayuda a evitar que los ciberdelincuentes tengan acceso a las credenciales de los empleados ya que estas pueden ser vulneradas de la siguiente manera, cuentas comprometidas por robo o contraseñas débiles.

» En la sede física de la organización, es importante emplear biométricos este dispositivo instalado en las todas las puertas principales como en cada área permite que una persona sea identificada y autenticada en base a datos reconocibles, verificables, únicos y específicos. Consiste en capturar un dato biométrico de la persona con intención de ingreso. Puede ser una foto de su rostro, un registro de su voz o una imagen de su huella digital.

Si esta persona tiene permiso temporal o indefinido de ingreso se compara con los datos biométricos de la persona que se va a autenticar. En TI, el control de acceso biométrico puede complementar la autenticación de usuarios y respalda las políticas de gestión de identidad y acceso (IAM) de las organizaciones.[7]

» Implementación del principio de menor privilegio (PoLP) es primordial ya que un usuario, aplicación o sistema recibe solo los niveles mínimos de acceso necesarios para realizar las tareas requeridas, y nada más. Es uno de los

[6] TREVINO, Aranza. Types of Multi-Factor Authentication (MFA). Keeper Security Blog - Cybersecurity News & Product Updates [página web]. (27, junio, 2023). [Consultado el 1, abril, 2024]. Disponible en Internet: <https://www.keepersecurity.com/blog/2023/06/27/types-of-multi-factor-authentication-mfa/>.

[7] VANIDAS, Mahanya. IAM authentication methods: Enterprise security. ManageEngine: IT security, operations & service management [página web]. (11, abril, 2022). [Consultado el 2, abril, 2024]. Disponible en Internet: <https://www.manageengine.com/academy/iam-authentication-methods.html>.

componentes centrales de Acceso a la Red de Confianza Cero (ZTNA) y una práctica fundamental en ciberseguridad.

Los entornos nativos de la nube a menudo se enfrentan a una base de usuarios en constante aumento y fluctuaciones esporádicas de recursos efímeros. La aplicación del principio de privilegio mínimo no es sólo una buena práctica, sino necesaria para mantener una postura de seguridad constante y eficaz. Esto requiere una configuración de entorno reflexiva y planificada previamente donde la seguridad y el cumplimiento puedan vivir junto con la productividad adecuada de los empleados y el acceso de los usuarios.[8]

Beneficios de esta práctica:

- Reduce la superficie de ataque
- Reducir la propagación de malware
- Reducir el error humano
- Lo mantiene preparado para cualquier auditoría

» Para soluciones Office 365, buscaría prevenir o detener la suplantación de identidad y phishing por correo electrónico, así como para mejorar la entrega por correo electrónico.

DMARC, DKIM y SPF son tres protocolos principales de seguridad de correo electrónico que ayudan a combatir el spam, el phishing y otros ataques basados en correo electrónico. A continuacion se detalla cómo funcionan usándolos para mejorar la seguridad de correo electrónico.[9]

---

[8] TRAN, Tim. How To Implement the Principle of Least Privilege. Keeper Security Blog - Cybersecurity News & Product Updates [página web]. (6, marzo, 2024). [Consultado el 31, marzo, 2024]. Disponible en Internet: <https://www.keepersecurity.com/blog/2024/03/06/how-to-implement-the-principle-of-least-privilege/#:~:text=To%20implement%20the%20principle%20of%20least%20privilege,%20organizations%20need%20to,and%20regularly%20audit%20network%20privileges.>.

[9] DMARC, DKIM, & SPF Explained (Email Authentication 101) - Valimail [Anónimo]. Valimail - DMARC SaaS Platform [página web]. (13, julio, 2023). [Consultado el 31, marzo, 2024]. Disponible en Internet: <https://www.valimail.com/blog/dmarc-dkim-spf-explained/>.

Aquí se indica una breve descripción de que es y cómo funciona.

SPF: Protocolo de autenticación de correo electrónico que ayuda a verificar que se envió un mensaje de correo electrónico desde un servidor autorizado. Funciona agregando un registro TXT a la configuración DNS de un dominio. Este registro especifica qué servidores están autorizados para enviar correo electrónico desde ese dominio. Cuando se recibe un correo electrónico, el servidor destinatario comprueba el registro SPF

DKIM: Protocolo de autenticación de correo electrónico. A diferencia de SPF, que verifica la autorización del servidor de envío, DKIM verifica la integridad del contenido del correo electrónico. Funciona agregando una firma digital al encabezado del correo electrónico. La firma se genera a través de una clave privada que solo el servidor de envío conoce.

DMARC: Proporcionar un sistema de autenticación de correo electrónico más robusto. Permite a los propietarios de dominios publicar políticas que especifican lo que debería suceder con los correos electrónicos que fallan las verificaciones de autenticación. La autenticación de mensajes, informes y conformidad basados en el dominio funcionan al agregar un registro TXT a la configuración de DNS de un dominio que especifica cómo manejar las comprobaciones SPF y DKIM fallidas.

» Para soluciones perimetrales es importante las listas de control de acceso (ACL) son una colección de permiso y negación restricciones, también conocidas como reglas, que ofrecen seguridad al evitar que usuarios no autorizados accedan a recursos particulares y otorgar acceso a usuarios autorizados. Además, las ACL pueden gobernar el flujo de tráfico, limitar la información en las actualizaciones de enrutamiento y determinar qué tipos de tráfico se envían o se niegan. Las ACL a menudo se sientan en un enrutador que actúa como un firewall o un enrutador que conecta dos redes internas.

- Delimitar países conocidos en el FW
- Identificación de dirección IP o de un rango de direcciones IP
- Pueden contener código SQL malicioso[10]

» Implementar XDR por sus múltiples beneficios este detectada una amenaza y otorga una puntuación de criticidad en función de la cual se realiza una acción específica, que también se puede programar para que se lleve a cabo posteriormente, o en el futuro reduciendo la cantidad de alertas relevantes, que de otro modo podrían pasarse por alto o considerarse como falsos positivos.

1.5 CONCLUSIONES QUE ORIENTEN ASPECTOS IMPORTANTES EN CUANDO A LA INVERSIÓN DE CIBERSEGURIDAD DENTRO DE LAS ORGANIZACIONES, DEBEN TENER EN CUENTA CADA UNA DE LAS ETAPAS QUE SE EJECUTARON A LO LARGO DEL SEMINARIO PARA PODER EJECUTAR ESTAS CONCLUSIONES Y SOPORTAR A LA ALTA GERENCIA LA NECESIDAD DE INVERSIÓN.

Mantener un alto nivel de confidencialidad es vital para respetar los acuerdos ya pactados entre las partes interesadas, pero es más importante denunciar actos ilegales y hacer cumplir leyes y regulaciones locales en las políticas colombianas. Descubrir irregularidades y respetar el acuerdo de confidencialidad no es argumento para no denunciar ante los organismos legales siendo este el puente para sancionar terceras personas y funcionarios corruptos, evasores y otros actores criminales sin importar el consentimiento del solicitante.

Irregularidades presentadas dentro de los acuerdos de confidencialidad es la de responder por el mal uso que le den sus representantes a la información confidencial. No debe ser responsabilidad de un individuo si representantes usan la información con intereses individuales los acuerdos confidenciales hacen hincapié

[10] ANYANWU, Chidiadi. What is An ACL? Access Control Lists Explained. freeCodeCamp.org [página web]. (14, abril, 2023). [Consultado el 31, marzo, 2024]. Disponible en Internet: <https://www.freecodecamp.org/news/a-deep-dive-into-access-control-lists/>.

en la buena fe de la persona que recibe la información y es quien debe hacer buen uso de esta, entendiendo siempre que el dueño y quien establece los acuerdos es la empresa. [11]

La principal ley que acoge los delitos cibernéticos es la 1273 de 2009

Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO: Un ejemplo de lo tratado a lo largo del seminario es poner en evidencia como un abogado autor del acuerdo confidencial fue despedido debido a que estuvo involucrado en actividades cuestionables, es comprensible que surja la preocupación de que el acuerdo de confidencialidad pueda haber sido redactado de manera no ética o incluso podría contener disposiciones que no sean legales o sean contrarias a los intereses de los expertos

Los activos son esencialmente cualquier cosa de valor que deba protegerse como por ejemplo los datos, aplicaciones, hardware, software e incluso personas. Son los componentes básicos de la infraestructura de cualquier organización, y sin la protección adecuada, son vulnerables a los ataques. Por lo anterior se debe tener en cuenta los artículos [12]

Artículo 269F. VIOLACIÓN DE DATOS PERSONALES.
Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS.

La ética es una disciplina un principio fundamental en la toma de decisiones haciéndolo un valor final en la todas las acciones propias realizadas. Las buenas acciones plasman las buenas conductas aprendidas en la infancia y estas serán

[11] ABOGADOS, navarro. Acuerdo de confidencialidad: qué es, cómo funciona y cómo se hace. Navarro Abogados [página web]. (3, julio, 2023). [Consultado el 19, febrero, 2024]. Disponible en Internet: <https://navarroabogados.net/acuerdos-confidencialidad-que-son/>.
[12] EL CONGRESO DE COLOMBIA. LEY 1273 DE 2009. https://www.sic.gov [página web]. (5, enero, 2009). [Consultado el 21, febrero, 2024]. Disponible en Internet: <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf>

aplicadas en toda etapa laboral. Toda parte interesada tiene la responsabilidad crucial de salvaguardar el bienestar, la salud y la seguridad del público. La seguridad es un imperativo ético que se debe mantener con un compromiso inquebrantable. Ya sea diseñando puentes o desarrollando dispositivos médicos, las consecuencias de pasar por alto las consideraciones de seguridad pueden ser nefastas. Equilibrar la protección de la información confidencial y la obligación ética de compartir conocimientos para el bien común hace parte de la toma de decisiones.[13]

» Crear conciencia sobre la ciberseguridad es bueno para todos, para mantener seguras a las personas y las redes, los empleados necesitan asesoramiento durante todo el año.
Ofrecer a las personas consejos útiles sobre cómo mantenerse seguros en línea (tanto en el trabajo como en todos los demás aspectos de la vida cotidiana) es algo bueno. Siempre habrá una carrera entre las compañías de software y los piratas informáticos cuando se descubre una nueva falla de seguridad, para ver si el proveedor puede solucionarlo antes de que los piratas informáticos puedan explotarlo. Pero dar a las personas incluso consejos básicos sobre cómo protegerse de los ataques contribuirá en gran medida a detener las infracciones.[14]

La realidad para muchas organizaciones es que sus usuarios son la primera y, a menudo, la última línea de defensa contra los ciberataques. Pero si no se les ha informado adecuadamente sobre lo que constituye estar seguro en línea, eso podría dejar a todos vulnerables.

Cosas como ataques de phishing y la importancia de utilizar una contraseña segura o incluso autenticación multifactor (MFA) son importantes para reducir el riesgo.

---

[13] CONSEJO PROFESIONAL NACIONAL DE INGENIERÍA. Código de ética | Copnia. Inicio | Copnia [página web]. (15, julio, 2015). [Consultado el 22, febrero, 2024]. Disponible en Internet: <https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica>.
[14] FASTERCAPITAL. Educar A Sus Empleados Sobre La Seguridad De La Red - FasterCapital. FasterCapital [página web]. (14, febrero, 2024). [Consultado el 3, abril, 2024]. Disponible en Internet: <https://fastercapital.com/es/tema/educar-a-sus-empleados-sobre-la-seguridad-de-la-red.html>.

» Con una solución SIEM, se logra:

Simplificar los informes de cumplimiento utilizando plantillas listas para auditorías y alertas de infracciones para reducir de manera efectiva el trabajo manual involucrado en la creación de informes y el monitoreo de eventos.

Reducir los falsos positivos y al mismo tiempo acelera la clasificación y la investigación de alertas legítimas, para que los SOC puedan centrarse en sus KPI. La automatización de los flujos de trabajo de respuesta para perfiles de alerta conocidos aumenta la cantidad de amenazas bloqueadas en las primeras etapas, lo que resulta en menos infracciones.
Reduce la probabilidad de una filtración de datos y reduzca el impacto de los ataques exitosos al reducir la cantidad de días que lleva detectar una filtración y recuperarse de ella.[15]

2. Sustenta el desarrollo de cada uno de los puntos plasmados en guía de la etapa 5 del seminario especializado mediante video donde se pueda evidenciar rostro del o la estudiante con una duración mínima de 15 minutos, el estudiante deberá hacer público el vídeo haciendo uso de alguna plataforma Cloud o en youtube.

https://www.youtube.com/watch?v=9ZoX4DUEKe4

[15] GOMEZ, Juan Armando. SIEM: Qué es y cómo puede optimizar la ciberseguridad de tu empresa. Home | Delta Protect [página web]. (25, julio, 2023). [Consultado el 3, abril, 2024]. Disponible en Internet: <https://www.deltaprotect.com/blog/siem-que-es>.

CONCLUSIONES

Los riesgos cibernéticos crecen de manera exponencial debido al valor incalculable de los datos personales y corporativos, la digitalización trae oportunidades como riesgos despreciables. Para mantener seguros los activos de información es importante estar actualizado y a la vanguardia de lo que trae el mercado, tener claridad en los nuevos vectores de ataque para agregar capas de seguridad dentro del entorno digital.

Red team se ha vuelto una herramienta fundamental para proteger a los sistemas frente a los ataques mal intencionados adoptan un enfoque integral del espectro completo de políticas, procesos y defensas de la organización para mejorar la preparación organizacional, mejorar la capacitación de los practicantes defensivos e inspeccionar los niveles de desempeño actuales de esta manera se puede mitigar los ataques perpetuados en las organizaciones.

Los Red Teams independientes han proporcionado información valiosa y objetiva sobre las vulnerabilidades y la eficacia de las defensas y los controles de mitigación que ya existen e incluso aquellos planificados para su futura implementación.

Por el otro lado, el equipo azul ha sido utilizado para auditar y validar la infraestructura de TI de las empresas, por medio de un plan determinara que impacto negativo tendra un ataque cibernético.

Los equipos azules comenzarían por desarmar y parchear el software para asegurarse de que los sistemas pudieran resistir un ataque cibernético. En algunos casos, el desarmado es breve, mientras que en algunos los equipos azules tendrían que restaurar todos los archivos en los servidores y corregir las vulnerabilidades. El atacante solo podrá identificar los objetivos y trabajar con solo una cantidad limitada de tiempo.

RECOMENDACIONES

Los países que lideran la lista entre los más afectados por ciberataques son Ecuador, Perú y Panamá con un promedio del 69% aproximadamente entre los tres países, generando en esta región un promedio de 35 ataques por segundo. Colombia no sale de esta lista y está relacionado en el top de países con intentos de infección y para ser exactos 87 por minuto.

Los expertos señalan como archivos con extensiones confiables como PDF resultan siendo troyanos que roban datos de tarjetas de crédito, códigos en sitios web donde el usuario ingresa sus credenciales siendo de esta manera una víctima más. Los shells web maliciosos son un tipo de software cargado en un servidor web comprometido para permitir el acceso remoto de un atacante. De qué manera los equipos blue team y red team pueden ayudar a los internautas a reducir las exposiciones a las vulnerabilidades buscando mejorar la defensa debido al crecimiento mundial que se ha tenido de ataques cibernéticos, que vectores se deben trabajar y mejorar para estar a la vanguardia y prevención de riesgos informáticos.

BIBLIOGRAFÍA

ABOGADOS, navarro. Acuerdo de confidencialidad: qué es, cómo funciona y cómo se hace. Navarro Abogados [página web]. (3, julio, 2023). [Consultado el 19, febrero, 2024]. Disponible en Internet: <https://navarroabogados.net/acuerdos-confidencialidad-que-son/>.

ANYANWU, Chidiadi. What is An ACL? Access Control Lists Explained. freeCodeCamp.org [página web]. (14, abril, 2023). [Consultado el 31, marzo, 2024]. Disponible en Internet: <https://www.freecodecamp.org/news/a-deep-dive-into-access-control-lists/>.

BUGCROWD. CIS Controls Framework (Center for Internet Security) | Bugcrowd. Bugcrowd [página web]. (16, agosto, 2022). [Consultado el 28, marzo, 2024]. Disponible en Internet: <https://www.bugcrowd.com/glossary/cis-controls-framework-center-for-internet-security/>.

CONSEJO PROFESIONAL NACIONAL DE INGENIERÍA. Código de ética | Copnia. Inicio | Copnia [página web]. (15, julio, 2015). [Consultado el 22, febrero, 2024]. Disponible en Internet: <https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica>.

EL CONGRESO DE COLOMBIA. LEY 1273 DE 2009. https://www.sic.gov [página web]. (5, enero, 2009). [Consultado el 21, febrero, 2024]. Disponible en Internet: <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf>

FASTERCAPITAL. Educar A Sus Empleados Sobre La Seguridad De La Red - FasterCapital. FasterCapital [página web]. (14, febrero, 2024). [Consultado el 3,

abril, 2024]. Disponible en Internet: <https://fastercapital.com/es/tema/educar-a-sus-empleados-sobre-la-seguridad-de-la-red.html>.

GIL, Marc Bolufer. Análisis completo de las ventajas y desventajas de Windows 10 Pro: ¿Vale la pena? - Ventajas y desventajas top. Ventajas y desventajas top [página web]. (2, noviembre, 2023). [Consultado el 29, marzo, 2024]. Disponible en Internet: <https://ventajasydesventajastop.com/windows-10-pro-ventajas-y-desventajas/>.

GOMEZ, Juan Armando. SIEM: Qué es y cómo puede optimizar la ciberseguridad de tu empresa. Home | Delta Protect [página web]. (25, julio, 2023). [Consultado el 3, abril, 2024]. Disponible en Internet: <https://www.deltaprotect.com/blog/siem-que-es>.

IBM. ¿Qué son los puntos de referencia de CIS? | IBM. IBM in Deutschland, Österreich und der Schweiz [página web]. (1, junio, 2024). [Consultado el 28, marzo, 2024]. Disponible en Internet: <https://www.ibm.com/es-es/topics/cis-benchmarks>.

KEEPCODING. ¿Qué es Purple Team en ciberseguridad? KeepCoding Bootcamps [página web]. (21, julio, 2023). [Consultado el 3, abril, 2024]. Disponible en Internet: <https://keepcoding.io/blog/que-es-purple-team-en-ciberseguridad/>.

ORDOÑEZ, Wilinton. Red Team, Blue Team y Purple team: Guía completa sobre los equipos en Ciberseguridad. Ciberseguridad, tecnología e innovación | GroupHacking [página web]. (23, julio, 2023). [Consultado el 2, abril, 2024]. Disponible en Internet: <https://www.grouphacking.com/ciberseguridad/hacking-etico/red-team-blue-team-y-purple-team-guia-completa-sobre-los-equipos-en-ciberseguridad/>.

TREVINO, Aranza. Types of Multi-Factor Authentication (MFA). Keeper Security Blog - Cybersecurity News & Product Updates [página web]. (27, junio, 2023). [Consultado el 1, abril, 2024]. Disponible en Internet: <https://www.keepersecurity.com/blog/2023/06/27/types-of-multi-factor-authentication-mfa/>.

SUMRAK, Jesse. DMARC, DKIM, & SPF Explained (Email Authentication 101) - Valimail [Anónimo]. Valimail - DMARC SaaS Platform [página web]. (13, julio, 2023). [Consultado el 31, marzo, 2024]. Disponible en Internet: <https://www.valimail.com/blog/dmarc-dkim-spf-explained/>.

TRAN, Tim. How To Implement the Principle of Least Privilege. Keeper Security Blog - Cybersecurity News & Product Updates [página web]. (6, marzo, 2024). [Consultado el 31, marzo, 2024]. Disponible en Internet: <https://www.keepersecurity.com/blog/2024/03/06/how-to-implement-the-principle-of-least-privilege/#:~:text=To%20implement%20the%20principle%20of%20least%20privilege,%20organizations%20need%20to,and%20regularly%20audit%20network%20privileges.>.

VANIDAS, Mahanya. IAM authentication methods: Enterprise security. ManageEngine: IT security, operations & service management [página web]. (11, abril, 2022). [Consultado el 2, abril, 2024]. Disponible en Internet: <https://www.manageengine.com/academy/iam-authentication-methods.html>.