Tipo de artículo: Artículo de revisión

UNIVERSIDAD DE LAS CIENCIAS INFORMÁTICAS

FACULTAD 2

Conformación de equipos para el control de la Ciberseguridad de manera eficiente y segura

Seminario de Gestión de la Ciberseguridad

Integrantes:

Erick Carlos Miralles Sosa:erickcms@estudiantes.uci.cu
Keylan Valdés García:keylanvg@estudiantes.uci.cu
Sheila Hernández Falcón:sheilahf@estudiantes.uci.cu
Sabrina D'Lory Ramos Barreto:sabrinadlrb@estudiantes.uci.cu
Marcos Daniel Artiles Delgado:marcosdad@estudiantes.uci.cu

Resumen

La conformación de un equipo de ciberseguridad es necesaria para la aplicación de buenas prácticas y medidas de seguridad informáticas en empresas e instituciones. Por lo que es necesario llevar a cabo un estudio sobre este tema,en la presente investigación se llevó a cabo una constante búsqueda el uso y utilización de las herramientas computacionales empleándose como gestor de fuentes bibliográficas el gestor Zotero.Principalmente las búsquedas de estas fuentes y referencias fueron realizadas en el sitiio Linkedin, Google , Google Scolar, en la Revista Cubana de Ciencias Informáticas y en los repositorios de la Universidad de Vallaolid, la Universidad Nacional Abierta y a Distancia de Bogotá y de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación de México. En la siguiente investigación se hará ver la importancia de la conformación de los equipos de ciberseguridad y la existencia de 3 equipos rojo,azul y morado.

Palabras Claves

Ciberseguridad,Conformación de Equipos, Equipo Rojo, Azul, Morado

Introducción

La evolución de la ciberseguridad como disciplina ha generado la necesidad imperante de organizar y estructurar el enfoque de protección de la información de manera más eficaz y especializada. Dada la amplitud y complejidad de los desafíos en materia de seguridad cibernética, se ha vuelto fundamental dividir el trabajo en equipos interdisciplinarios, cada uno con roles específicos, con el propósito de lograr una mayor eficiencia y escalabilidad en el manejo de la seguridad de la información.

Para la separación del trabajo de la ciberseguridad surgieron tres grupos dedicados a abordar distintos aspectos de la ciberseguridad, los denominados equipos rojo,azul y morado

Este trabajo tiene como objetivo principal definir y explicar las técnicas utilizadas en la conformación de equipos de ciberseguridad, detallando la función de cada grupo.Además, se abordará en detalle las responsabilidades específicas de cada uno de los equipos, las herramientas fundamentales que deben ser implementadas en su labor diaria, y las vulnerabilidades críticas que deben ser erradicadas para garantizar la protección integral de los activos y datos de una organización frente a las crecientes amenazas cibernéticas.

Desarrollo

Las empresas a menudo tienen que preguntarse si tiene sentido contratar a un experto externo para mantener su integridad. Ya sea perfeccionando sus procesos de recursos humanos, administrando comunicación con los clientes y marketing o creando un equipo interno para gestionar estas operaciones complejas.(Infosecurity,junio 2023).La conformación de equipos de ciberseguridad implica una serie de combinación de técnicas y enfoques para enfrentar las amenazas cibernéticas.(SANS Institute,2019)

1. **Identificación de habilidades y roles:** Se realiza un análisis de las habilidades necesarias para proteger los activos digitales de una organización

2. **Contratación y reclutamiento**: Se busca a profesionales con las habilidades y experiencia necesarias para formar parte del equipo de ciberseguridad. Esto puede implicar la contratación de personal interno o la búsqueda de talento externo a través de agencias especializadas o plataformas de reclutamiento.

3. **Formación y capacitación:** Se brinda capacitación continua a los miembros del equipo para mantenerse actualizados sobre las últimas amenazas y técnicas de ciberseguridad. Esto puede incluir cursos, talleres, certificaciones y participación en conferencias y eventos relacionados con la ciberseguridad.

4. **Colaboración y trabajo en equipo:** Se fomenta la colaboración entre los miembros del equipo para compartir conocimientos, ideas y mejores prácticas. Esto puede incluir reuniones regulares, sesiones de lluvia de ideas y grupos de estudio.

5. **Implementación de marcos y estándares de seguridad:** Se utilizan marcos y estándares reconocidos en la industria, como ISO 27001, NIST Cybersecurity Framework o CIS Controls, para guiar las prácticas de

seguridad del equipo. Estos marcos proporcionan una estructura y lineamientos para la gestión de riesgos y la implementación de controles de seguridad.

Existen diferentes métodos a emplear en la conformación de estos equipos pues un sólido equipo de ciberseguridad debe estar conformado por distintos miembros. Cada uno con un perfil y rol específico.Antes de armar los equipos se debe tener en cuente objetivo de la empresa, presupuesto,el tipo de base de datos y sotware.(Serra,Juan,2022)

La lista de roles que deben existir en el control de la seguridad son:

- **Analista de seguridad de datos:**El analista de seguridad de datos, es la primera defensa de los sistemas y redes de la organización . Ataques, tanto contra las redes internas, como contra las estructuras generales de los sistemas, buscando proteger los archivos y datos de la compañía y de los mismos clientes. Este tipo de profesional se encargarse de tareas importantes, críticas. Tales como auditorías de seguridad, análisis de riesgos, detección de vulnerabilidades, desarrollo de políticas de ciberseguridad y procedimientos de seguridad general.

- **Gestor de seguridad de sistemas de información:**Se encarga de administrar las medidas de ciberseguridad de la empresa. Esto incluye tanto la implementación de políticas y prácticas de ciberseguridad, así como también la supervisión del armado y funcionamiento de las estructuras generales de seguridad informática.

- **Arquitecto de Seguridad:**Responsables de encontrar formas de proteger los sistemas de las amenazas que existen en la red. En los equipos de ciberseguridad, será la persona que intente penetrar los propios sistemas, buscando siempre generar nuevas protecciones, testearlo y mejorarlo.De esta , luego recomiendan optimizaciones y mejoras a las personas encargadas de aplicar los software y las políticas de seguridad en general.

- **Pentester:**No confundir con Arquitecto de Seguridad pues este se dedica a realizar “pruebas de penetración” simulando ataques reales. Estos son confundidos muchos veces pensando que son parte de los llamados Red Team ,(Coursera Staff diciembre 2023),pues los pentester solo forman parte del equipo en un período determinado , mientras que los Red Team son parte oficial de este(SeguInfo,noviembre de 2019)..

Para la separación de estos roles y el logro de mejores resultados como se dejó escrito anteriormente inicialmente se dividían estos equipos de ciberseguridad en 2 “subqeuipos” Red Team y Blue Team.

Red Team

El Red Team es el que nombramos seguridad ofensiva y está formado por profesionales de la seguridad que actúan como adversarios para superar los controles de ciberseguridad. Se encarga de poner a prueba el Blue Team buscando vulnerabilidades.(Martha Paredes,mayo2023).

El primer paso de este equipo es recopilar, comprender y analizar las amenazas que podría presentar cada institución,obteniendo información sobre las últimas vulnerabilidades,malware,exploits y técnicas de ataque usadas por ciberdelincuentes, además identificando las técnicas,tácticas y procedimientos(TTPs) (Sudheer Kumar,septiembre 2023) que usan los advesarios para comprometer la red y los sistemas.Esto es realizado por los analistas de amenazas.

Los Red Team, aunque no lo parezca, pasan más tiempo planificando un ataque que realizando ataques. De hecho, el Red Team se encarga de implementar una serie de métodos para obtener acceso a una red. Se contrata el Red Team para probar la efectividad del equipo azul emulando los comportamientos de un equipo negro real (ciberatacantes) para que el ataque sea lo más realista y caótico posible.((Martha Paredes,mayo2023).

Estos usuarán todos lo disponible y necesario tanto como métodos y herramientas para explotar las debilidades y vulnerabilidades usando técnicas como phsihing,identificación de vulnerabilidades,inntrusión de firewall.

Metodología Red Team

♦ **Definición y planificación**: Se define qué tipo de vectores o activos críticos serán utilizados y de qué manera serán atacados.

♦ **Reconocimiento externo:** Consiste en desarrollar todas las acciones posibles para identificar los activos que están expuestos en el ámbito que se vaya a comprobar.

♦ **Compromiso inicial:** Se identifica una vulnerabilidad lo suficientemente crítica que permita abrir paso a la intrusión.

♦ **Acceso a la red interna:** Una vez se compromete un primer activo, se debe buscar el camino y la forma para acceder a la red interna.

♦ **Elevación de privilegios:** En esta etapa del ejercicio se busca crear vías de acceso secundarias en caso que el Blue Team detecte el ataque al vector principal y lo detenga.

♦ **Reconocimiento interno:** Cuando se tiene acceso pleno a toda la organización, lo primero que se debe hacer es un reconocimiento interno de todos los activos para evaluar cuáles podrían ser los ataques más radicales que se puedan hacer.

Vectores de acceso

La forma que tiene el Red Team para acceder a las vulnerabilidades puede ser a través del uso de cualquier sistema expuesto a internet a través de esos activos o mediante una infraestrucutra wifi, también el análisis de usb para detectar malware, el Spear PHishing para a través de suplantación de comunicaciones acceder a la información de la institución y por último una práctica más extrema sería ingresar de forma presencial buscando posibles fallas(Martha Paredes,mayo2023).

Blue Team

Ahora bien si en resumen se puede decir que los Red Team descubren las fallas y vulnerabilidades quien lleva a cabo la solución de estas es el conocido equipo azul.El Blue Team es el encargado de la seguridad defensiva y se forma por profesionales de la ciberseguridad con el fin de salvaguardar activos críticos

El principal objetivo del Blue Team es realizar evaluaciones de las distintas amenazas que puedan afectar a las organizaciones, monitorizar (red, sistemas, etc.) y recomendar planes de actuación para mitigar los riesgos. Además, en casos de incidentes, realizan las tareas de respuesta, incluyendo análisis de forense de las máquinas afectadas(Unir Noticias ,enero de 2020)

Funciones del blue team

- Realizan una vigilancia constante, analizando patrones y comportamientos que se salen de lo común tanto a nivel de sistemas y aplicaciones como de las personas, en lo relativo a la seguridad de la información.
- Trabajan en la mejora continua de la seguridad, rastreando incidentes de ciberseguridad, analizando los sistemas y aplicaciones para identificar fallos y/o vulnerabilidades y verificando la efectividad de las medidas de seguridad de la organización

Metodología

El primer paso que realiza el Blue Team es la realización de una vigilancia constante con el análisis de patrones y compartamientos,además trabajan en la mejora continua de la seguridad, rastreando incidentes de ciberseguridad, analizando los sistemas y aplicaciones, dado que no siempre el equipo rojo colabara con el azul este también tiene que tomar todas las medidas para responer una intrusión.Por lo que este equipo siempre es necesario en el

control de la ciberseguridad con el objetivo de garantizar la seguridad de una organización a largo tiempo

Características

- Ser un equipo multidisciplinar
- Focalizarse en prestar servicios de seguridad defensiva personalizados a las características y recursos de la empresa
- Enfocar la seguridad desde dentro de la organización
- Realizar un trabajo proactivo y continuo
- Conocer las características de la empresa para conjugar los intereses de negocio con los objetivos de seguridad

Purple Team

Para un correcto funcionamiento y control de la seguridad informática es necesario que haya una fluida comunicación entre los red y blue team pero por problemas de desconocimientos de metodologías del otro equipo, rivalidad no sana o propiamente por desorganización de la institución esa comunicación falle, surgiendo de esta manera el Purple Team.

Metodología del Purple Team

El Purple Team actúa como un puente entre el Red Team (equipo de ataque) y el Blue Team (equipo de defensa), facilitando la cooperación y el intercambio de conocimientos y enfoques. Su metodología es basaba a través:

- Simulación de ataques controlados: Se realizan simulaciones de ataques en las que el Red Team ejecuta tácticas de ataque reales, mientras que el Blue Team responde y defiende la red como lo haría en una situación real.

- Debriefings y análisis conjunto: Después de cada simulación, el Purple Team facilita sesiones de debriefing en las que ambos equipos revisan los resultados, comparten conocimientos, identifican vulnerabilidades y áreas de mejora, y establecen planes de acción.

Funciones del Purple Team:

- Promueve una comunicación efectiva y colaborativa entre el Red Team y el Blue Team,.
- Colaboración en el Análisis de Resultados
- Desarrolla planes de mejora basados en los hallazgos y lecciones aprendidas de las simulaciones.
- Proporciona recomendaciones para fortalecer la infraestructura de seguridad y los procesos de respuesta a incidentes.
- Resuelve el problema del desconocimiento de metodologías de un equipo respecto a otra pues proporciona capacitación y desarrollo de habilidades a ambos equipo

También el Purple Team puede ser usado como un híbrido en empresa o instituciones con pocos recursos, cumpliendo este equipo las funciones de esos otros dos.

Otros equipos de menor relevancia o subequipos que pueden existir en una institución son:

Threat Hunting:Esta subdivisión del Equipo Azul se encarga, como su nombre indica, de la búsqueda activa de amenazas para aislarlas de los sistemas que buscamos proteger. Lo que diferencia a este equipo del Blue Team es la proactividad en la búsqueda de posibles ciberataques. Las otras estrategias de defensa se basan, sobre todo, en la detección y respuesta de ataques, posteriormente a que hayan sucedido.

CERT **Computer Emergency Response Team (CERT)** se especializa en **r**esponder ante ataques y amenazas. Puede considerarse también como una rama del Equipo Azul encargada de solucionar incidentes. Un ejemplo de uno de estos equipos es el CERT del Centro de Criptología Nacional de España, el cual organiza cursos y juegos de CTF para la comunidad de la ciberseguridad.

***CSIRT* El Computer Security Incidents Response Team (CSIRT),** al igual que el CERT, también es un equipo de respuesta a incidentes. Sin embargo, estos aplican, sobre todo, para los gobiernos, la política y el mundo de los negocios.

Conclusiones

Con el estudio sobre la conformación de equipos de ciberseguridad podemos arribar a las siguientes conclusiones:

- Las instituciones deben diseñar e implementar medidas de seguridad para lograr la erradicación de la mayor cantidad de ataques.
- Los equipos rojos y azules son la opción fundamental para propocionar una correcta seguridad informática en las instituciones.
- Igual importancia puede tener el equipo morado pues el que permite la comunicación entre estos y permite sustituir a ambos si no se cuenta con los recursos necesarios
- Los equipos de ciberseguridad siempre pueden variar en cantidad y trabajo específico según el tamaño de la empresa, incluso existen otros equipos menores y subequipos como:*Threat Hunting: y CERT*

Referencias Bibliográficas

1. Coursera Staff<<How to Become a Penetration Tester: 2024 Career Guide>> 15 diciembre de 2023

2. González Gustavo Alfonso <<CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA LOS EQUIPOS REDTEAM Y BLUETEAM EN COLOMBIA>> 2021
3. Infosecurity <<Cómo armar un equipo de ciberseguridad para tu empresa>>octubre de 2023
4. Martha Paredes <<¿Sabias que hay equipos específicos para ciberseguridad?,Linkedin>> 2-5-2023

5. Penetration Testing vs. Red Teaming ¿Cuál es la diferencia?
6. SANS Institute<<Building an Effective Cybersecurity Team SANS Institute>> 2019
7. Serra Juan <<Equipos de ciberseguridad: Cómo se conforman>>29-6-2022
8. Segu Info<<Penetration Testing vs. Red Teaming ¿Cuál es la diferencia?>>12-11-2019
9. Sudheer Kumar <<Tactics, Techniques, and Procedures (TTPs) In Cyber Threat Intelligence, Linkedin>>26-9-2023

10. Unir Noticias <<Red team, Blue team y Purple team,cuáles son sus funciones y diferencias>>7-1-2020