MARIANO ALFONSO.
CIBERSECURITY STUDENT | CTF PLAYER

Basic concepts of Cybersecurity

McCumber Cube and CIA Triad

BLOG
0mariano.github.io

14 de Febrero del 2024

Índice

1. Introducción

En este Artículo, nos adentraremos en dos pilares fundamentales del campo de la seguridad informática: la Triada CIA y el Cubo de McCumber. Estos conceptos son esenciales para comprender cómo proteger la información y los sistemas contra amenazas y ataques.

El objetivo de este artículo no solo es proporcionar una comprensión básica de estos conceptos fundamentales, sino también fomentar la colaboración y el intercambio de conocimientos dentro de la comunidad de la **CiberSeguridad**, **Pentesting**, **Hacking Ético**.

2. McCumber Cube

En *1991*, **John McCumber** lanzó un modelo de riesgo de ciberseguridad conocido como el cubo de McCumber. Este modelo fue revolucionario por la forma en que describía los *factores de riesgo de ciberseguridad* como un cubo tridimensional. Cada una de las caras visibles del cubo tiene tres aspectos diferentes del riesgo en ciberseguridad que deben gestionarse.

Los aspectos de cada dimensión son:

1. Los principios fundamentales para proteger los sistemas de información.
2. La protección de la información en cada uno de sus estados posibles.
3. Las medidas de seguridad utilizadas para proteger los datos.

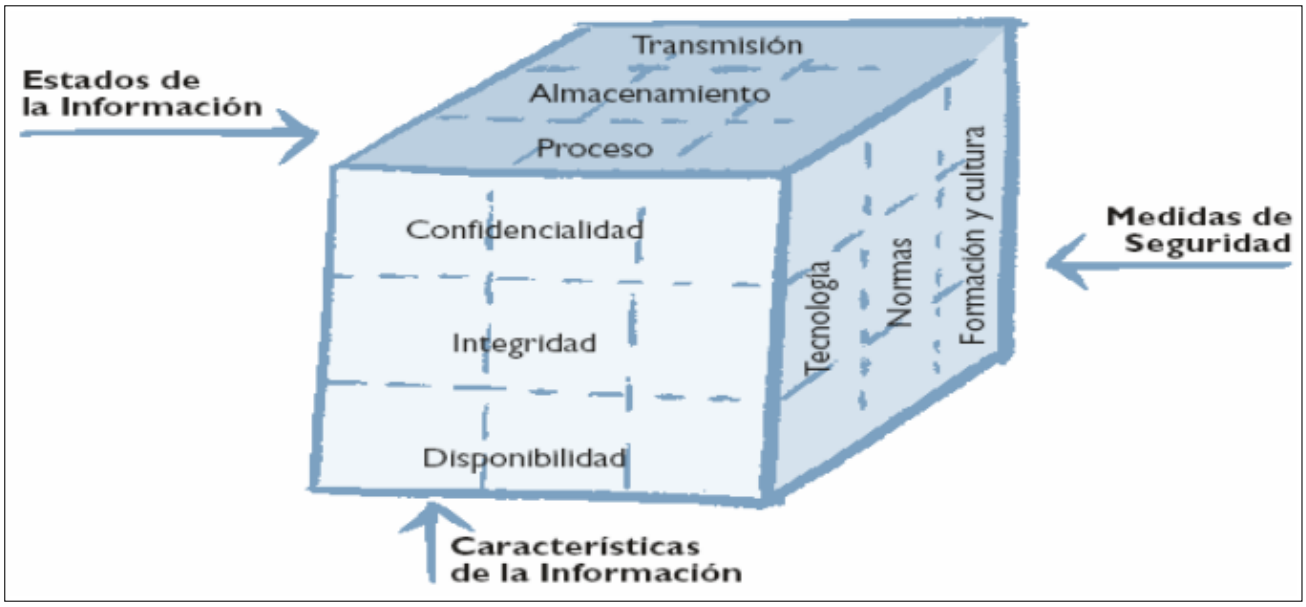

Figura 1: Cubo McCumber.

3. Los principios fundamentales para proteger los sistemas de información

3.1. Triada CIA

Cuando nos referimos a la **Triada CIA**, estamos hablando de los conceptos de *Confidencialidad*, *Integridad* y *Disponibilidad* (por sus siglas en inglés Confidentiality, Integrity, Availability). Es fundamental comprender el significado de estas palabras para desarrollar políticas y protocolos de seguridad informática que no solo protejan la información de posibles ataques de ciberdelincuentes, sino también al usuario al que pertenecen estos datos o que busca hacer uso de los mismos.

Figura 2: Triada CIA.

3.1.1. Confidencialidad

Consiste en evitar que la información sensible sea revelada a personas no autorizadas, es decir, la información debe mantenerse en secreto y no debe divulgarse. De lo contrario, el pilar de confidencialidad de la Triada CIA se corrompería.

Ejemplo:

Un claro ejemplo sería aquellas personas que trabajan en RR.HH. y manejan hojas de cálculo, cuentas bancarias, recibos de sueldo u otra información relacionada con el flujo de dinero. Por ello, no se otorgan permisos de acceso a la gran mayoría de otros empleados, y quizás incluso a ciertos ejecutivos. Si una organización tiene empleados que no pertenecen al área de RR.HH. y tienen acceso a cierta información a la que no deberían tener acceso, el pilar de confidencialidad no se cumple.

Los métodos utilizados para garantizar la confidencialidad incluyen el **cifrado de datos**, la **autenticación** y el **control de acceso físico**.

3.1.2. Integridad

Garantiza que la información sea confiable, consistente y precisa, protegiéndola contra modificaciones o alteraciones intencionales o accidentales, independientemente de cuánto tiempo haya pasado desde su creación. Si se protege la integridad de la información, se garantiza su confiabilidad y precisión.

Ejemplo:

Una entidad bancaria debe garantizar que los datos de sus clientes no sean modificados o manipulados. Garantizar la integridad implica proteger los datos en uso, en tránsito (por ejemplo, al enviar un correo electrónico o al cargar o descargar un archivo) y al almacenarlos.

Una forma de garantizar la integridad es utilizar **firmas digitales**.

3.1.3. Disponibilidad

Garantiza que la información esté disponible o accesible para personal autorizado siempre, cuando y donde sea necesario. Es decir, la capacidad de proporcionar acceso oportuno e ininterrumpido a los objetos depende tanto de la integridad como de la confidencialidad; sin ninguna de ellas, este pilar no se cumple.

Ejemplo:

Supongamos que una empresa utiliza un sistema de gestión de inventario para llevar un registro preciso de su inventario y procesar pedidos de manera eficiente. Si este sistema experimenta una interrupción debido a un ataque, un error de hardware o un desastre natural, la disponibilidad se verá comprometida. Como resultado, los empleados no podrán acceder al sistema para realizar pedidos.

La disponibilidad se puede proteger mediante el **mantenimiento** de los **sistemas operativos**, **actualizaciones de software** y **creando copias de seguridad**, así como la **implementación** o utilización de **servidores de alta disponibilidad**.

Lograr que los tres elementos estén en equilibrio puede ser un desafío, pero idealmente, cuando se cumplen los tres pilares, el perfil de seguridad de la organización es más sólido y está mejor equipado para manejar incidentes de amenazas.

4. La protección de la información en cada uno de sus estados posibles

4.1. Procesamiento

Se refiere a los datos que se utilizan para realizar una operación como la actualización de un registro de base de datos (datos en proceso)

4.2. Almacenamiento

Se refiere a los datos almacenados en la memoria o en un dispositivo de almacenamiento permanente, como un disco duro, una unidad de estado sólido o una unidad USB (datos en reposo)

4.3. Transmisión

Se refiere a los datos que viajan entre sistemas de información (datos en tránsito)

5. Las medidas de seguridad utilizadas para proteger los datos

5.1. Awareness

Una organización debe implementar medidas de concientizacion mediante capacitaciones y educación sobre los empleados para que estén informados sobre las posibles amenazas a la seguridad y las acciones que pueden tomar para proteger los sistemas de información.

5.2. Tecnología

Se refiere a las soluciones basadas en software y hardware diseñadas para proteger los sistemas de información como los firewalls, que monitorean continuamente su red en busca de posibles incidentes maliciosos.

5.3. Políticas y el procedimientos

Se refiere a los controles administrativos que proporcionan una base para la forma en que una organización implementa el aseguramiento de la información, como los planes de respuesta a incidentes y las pautas de mejores prácticas.

6. Apéndice I Links de Referencia

6.1. Documentación

- **Cisco: Introducción a la Ciberseguridad**
  https://skillsforall.com/course/introduction-to-cybersecurity?courseLang=en-US
- **Wikipedia: McCumber cube**
  https://en.wikipedia.org/wiki/McCumber_cube
- **IBM: Conservación de la protección de datos en el mundo de la multicloud híbrida**
  https://www.ibm.com/downloads/cas/OZ26LOBW
- **Fortinet: Tríada CIA: confidencialidad, integridad y disponibilidad**
  https://www.fortinet.com/lat/resources/cyberglossary/cia-triad

7. Contacto

E-mail: **marianoalfonso80@protonmail.com**

LinkedIn: **https://www.linkedin.com/in/mariano-alfonso-667a60226**

Blog: **https://0mariano.github.io**

GitHub: **https://github.com/0mariano**