CrowdStrike

Fallo de Confidencialidad en Seguridad Informática

Comisión 15 - POPP Franco, SCHWERDT Matias

Seguridad informatica: CIA

La Tríada CIA es un modelo que define los tres principios clave para proteger la información en seguridad informática:

- Confidencialidad
- Integridad
- Disponibilidad.

Confidencialidad y Seguridad

- La confidencialidad asegura que solo personas autorizadas puedan acceder a la información.

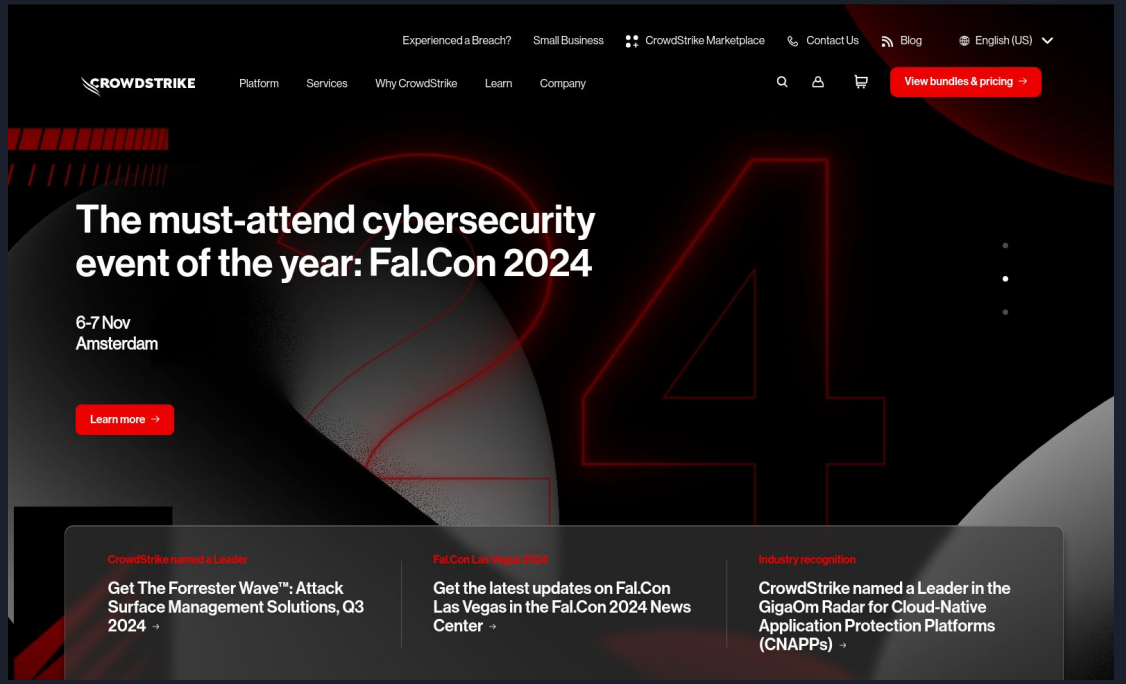
- Es muy importante para proteger datos sensibles y mantener la confianza en sistemas y empresas.

Ejemplos de Fallos de Confidencialidad

- **Filtración de Datos Personales**: una empresa sufre un **ciberataque** y expone información.
- **Acceso No Autorizado**: por ej. un **empleado** de una empresa accede a información confidencial sin permisos
- **Phishing**: se engaña a los usuarios para que compartan sus credenciales
- **Errores de configuración**: un servidor o una bdd mal configurados permiten el acceso público sin necesidad de autenticación

¿Qué es CrowdStrike?

CrowdStrike es una empresa de **ciberseguridad** que desarrolla software para proteger contra amenazas y ataques de malware. Su producto principal, **Falcon Sensor,** es ampliamente usado en empresas y organizaciones.



El Incidente de CrowdStrike

El 19 de julio de 2024, una actualización defectuosa de su software de seguridad, Falcon Sensor, afectó a millones de sistemas Windows.

Aproximadamente 8,5 millones de computadoras no pudieron reiniciarse correctamente, marcando una de las mayores interrupciones en la historia de la tecnología de la información.

El incidente destaca la importancia de la seguridad en sistemas críticos y las graves consecuencias de un fallo de confidencialidad.

Posibles Consecuencias en la Confidencialidad

Sin la protección activa de CrowdStrike, los sistemas quedaron **expuestos a posibles ataques**.

Los atacantes podrían haber aprovechado esta **vulnerabilidad para acceder a datos confidenciales**.

Los sistemas afectados no podían reiniciarse adecuadamente, lo que llevó a muchos equipos a quedar en un estado de **inactividad o reinicio continuo**.

Este tipo de fallo hace que los sistemas estén más expuestos, ya que los administradores de TI pueden recurrir a soluciones de emergencia o procedimientos alternativos, como desactivar ciertas protecciones para intentar recuperar el control de los sistemas.

Solución

CrowdStrike lanzó un **parche de emergencia** para solucionar el problema, pero en algunos casos fue necesario aplicar el parche en modo seguro o usando herramientas de administración de emergencia.