ELECTIVA: Habilidades practicas en el ciberespacio

INCIDENTE CROWDSTRIKE

MY RAMIRO ALVARADO REYES
MY. RAFAEL AUGUSTO GIRALDO RESTREPO
MY. RAFAEL ALBERTO MARTINEZ MARTINEZ
MY. JAIME ALBERTO PATIÑO ROMERO

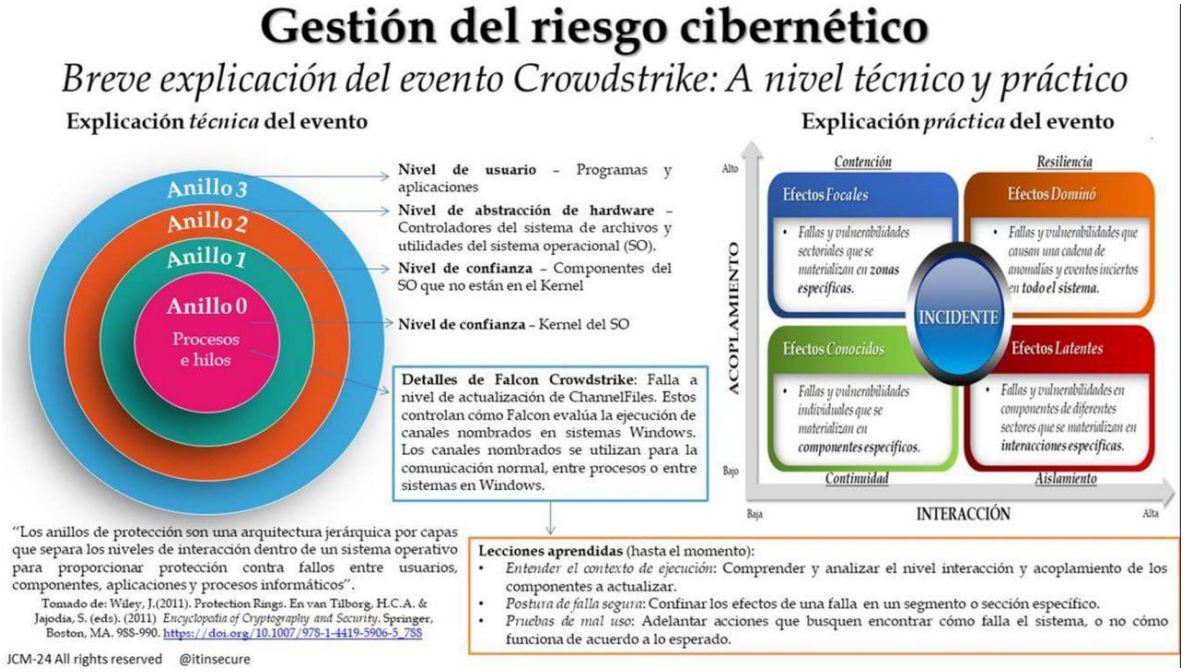
El incidente de CrowdStrike ocurrió en el mes de julio de 2024, causado por una actualización defectuosa en su software de seguridad Falcon, lo que llevó a una interrupción masiva de TI a nivel mundial. La actualización, lanzada el 19 de julio, contenía un error que provocó que aproximadamente 8.5 millones de computadoras con Windows fallaran y no pudieran reiniciarse correctamente. Este problema afectó a bancos, aerolíneas, hospitales y otras industrias en más de 20 países.

El fallo se debió a una prueba defectuosa en el proceso de actualización rápida de CrowdStrike, diseñada para responder rápidamente a nuevas amenazas de ciberseguridad. La compañía ha prometido mejorar sus procesos de prueba para evitar que incidentes similares ocurran en el futuro, incluyendo pruebas más rigurosas y la implementación de técnicas avanzadas como pruebas de reversión y pruebas de esfuerzo.

La recuperación del incidente implicó reiniciar las máquinas afectadas varias veces, a menudo conectadas a la red para descargar un archivo de reversión. En algunos casos, fue necesario iniciar en modo seguro y eliminar manualmente archivos específicos. Este proceso fue laborioso y tomó varios días para que las empresas afectadas pudieran restaurar todos sus sistemas.

El incidente tuvo un impacto global significativo, afectando a bancos, aerolíneas y hospitales. Estas interrupciones resultaron en la cancelación de más de 5,000 vuelos y graves problemas operativos en múltiples sectores. Las pérdidas financieras se estimaron en $5.4 mil millones.

ELECTIVA: Habilidades practicas en el ciberespacio



La arquitectura de los anillos de protección en sistemas operativos es un modelo de gestión de privilegios que se utiliza para mejorar la seguridad y la estabilidad del sistema. Este modelo segmenta las operaciones y recursos del sistema en diferentes niveles de privilegio, denominados "anillos", donde cada anillo tiene un nivel de autoridad y acceso diferente. Aquí te explico los anillos de protección más comunes:

Anillo 0 (Kernel Mode)

- **Propósito:** Este es el anillo con el nivel más alto de privilegio y control absoluto sobre el hardware.
- Acceso: Tiene acceso directo al hardware, a la memoria y a todos los recursos del sistema.
- **Componentes:** Contiene el núcleo del sistema operativo (kernel), controladores de dispositivos y otros componentes críticos.
- **Riesgo:** Un fallo en este nivel puede causar un colapso total del sistema.

ELECTIVA: Habilidades practicas en el ciberespacio

Anillo 1 (Supervisor Mode)

- **Propósito:** Se utiliza para ejecutar algunos servicios del sistema y tareas que requieren más privilegios que las aplicaciones de usuario.
- **Acceso:** Acceso restringido en comparación con el anillo 0, pero puede gestionar recursos del sistema y realizar tareas de bajo nivel.
- **Componentes:** Puede incluir ciertos controladores y servicios del sistema operativo.

Anillo 2 (System Mode)

- **Propósito:** Maneja funciones del sistema que requieren menos privilegios que las del anillo 1.
- **Acceso:** Tiene acceso limitado a los recursos del sistema.
- **Componentes:** Generalmente contiene servicios del sistema y funciones utilitarias que no necesitan acceso total al hardware.

Anillo 3 (User Mode)

- **Propósito:** Es el anillo con el nivel de privilegio más bajo, donde se ejecutan las aplicaciones de usuario.
- **Acceso:** No tiene acceso directo al hardware ni a la memoria del sistema, limitándose a usar interfaces y servicios proporcionados por los anillos superiores.
- **Componentes:** Aplicaciones de usuario como navegadores web, procesadores de texto y otros programas.

Funcionamiento General

- **Transiciones:** La comunicación entre los anillos se realiza a través de llamadas al sistema (system calls), que permiten a las aplicaciones de usuario solicitar servicios del núcleo.
- **Protección:** Este modelo ayuda a proteger el sistema operativo de errores y ataques, ya que limita el acceso directo al hardware y recursos críticos a los componentes más confiables y menos susceptibles a fallos.

ELECTIVA: Habilidades practicas en el ciberespacio

Explicación técnica del evento:

Según la imagen proporcionada, el incidente de CrowdStrike ocurrió en el Anillo 0, que es el nivel más privilegiado del sistema operativo, conocido como el kernel. El Anillo 0 tiene control total sobre todos los recursos del sistema, incluyendo la memoria y el hardware, y maneja los procesos e hilos críticos. La falla mencionada en los detalles del evento se refiere a una actualización de ChannelFiles, que controla cómo Falcon evalúa la ejecución de canales nombrados en sistemas Windows. Este tipo de control profundo y directo con el núcleo del sistema operativo es consistente con las operaciones del Anillo 0.

El Anillo 0, al ser responsable de gestionar todas las operaciones críticas del sistema, implica que cualquier falla en este nivel puede comprometer seriamente la integridad y la seguridad del sistema operativo. La interacción directa con el kernel y la naturaleza crítica de los ChannelFiles, que afectan la evaluación y ejecución de procesos en Windows, refuerzan que la ubicación de la falla está en el Anillo 0. Por lo tanto, es correcto concluir que el incidente de CrowdStrike se produjo en el Anillo 0 del sistema operativo.

Explicación practica del evento:

La sección "Explicación práctica del evento" del diagrama nos muestra de manera clara y concisa cómo se pueden gestionar y entender los diferentes tipos de problemas que pueden surgir durante un incidente cibernético. Esta sección está dividida en cuatro cuadrantes, cada uno representando una combinación de contención e interacción que ayuda a categorizar las fallas y vulnerabilidades. Esta información es esencial para comprender el impacto de un incidente y planificar la mejor manera de responder.

Los "Efectos Focales" se refieren a problemas específicos que afectan solo a ciertas áreas del sistema. Debido a que estos problemas están contenidos en una zona específica, es más fácil manejarlos y resolverlos sin que se propaguen. La baja interacción de estos efectos significa que no se extienden a otras partes del sistema, lo que permite a los equipos de seguridad abordarlos de manera más directa y efectiva.

En comparación, los "Efectos Conocidos" son problemas que ya se han identificado y que afectan a componentes específicos del sistema. Aunque pueden no estar tan contenidos como los efectos focales, su baja interacción implica que no se propagan fácilmente a otras áreas. Estos efectos son bien entendidos por los equipos de seguridad, lo que facilita su identificación y corrección, aunque es importante mantener una vigilancia constante para evitar que se conviertan en problemas mayores.

Los "Efectos Dominó" y los "Efectos Latentes" representan desafíos más complejos. Los "Efectos Dominó" son especialmente peligrosos porque una falla inicial puede desencadenar una serie de problemas en cascada que afectan a múltiples áreas del sistema debido a su alta interacción y baja contención. Por otro lado, los "Efectos Latentes" pueden estar contenidos una vez identificados, pero necesitan ciertas condiciones para manifestarse y tienen alta interacción, lo que significa que pueden influir en varios componentes del sistema. Estos tipos de efectos destacan la importancia de una monitorización constante y una preparación proactiva para mitigar los impactos antes de que se conviertan en problemas significativos. Entender estas categorías ayuda a los equipos de seguridad a diseñar estrategias más efectivas para proteger el sistema y asegurar su resiliencia ante futuros ataques.

Lecciones aprendidas:

Una de las lecciones aprendidas más importantes del evento de CrowdStrike es la necesidad de entender el contexto de ejecución de los componentes del sistema. Antes de realizar cualquier actualización, es crucial analizar cómo interactúan y se acoplan los distintos componentes. Este conocimiento profundo permite anticipar posibles impactos y conflictos que puedan surgir durante las actualizaciones, asegurando que se realicen de manera segura y efectiva. Sin esta comprensión, las actualizaciones pueden introducir vulnerabilidades no anticipadas que podrían comprometer la seguridad del sistema.

Otra lección clave es adoptar una postura de falla suave, que implica diseñar el sistema para manejar los fallos de manera controlada y limitar su impacto a segmentos específicos. Esto se logra implementando mecanismos de contención que eviten la propagación de fallas a

través del sistema. Controlar los efectos de una falla en un segmento específico es crucial para mantener la estabilidad y seguridad operativa. Una estrategia de falla suave minimiza el impacto de los errores y facilita una recuperación más rápida, protegiendo así la integridad del sistema.

Finalmente, es fundamental evitar operar en modo aislado, lo que significa no limitarse a observar el sistema solo cuando todo está funcionando bien. Es esencial realizar pruebas y análisis proactivos para identificar posibles fallas y vulnerabilidades antes de que ocurran. Esta aproximación preventiva permite a los equipos de seguridad entender mejor los puntos débiles del sistema y prepararse adecuadamente para mitigar riesgos potenciales. Al buscar activamente cómo puede fallar el sistema, en lugar de solo observar su funcionamiento esperado, se fortalece la capacidad de respuesta y recuperación ante cualquier incidente, mejorando así la resiliencia general del sistema.

ELECTIVA: Habilidades practicas en el ciberespacio

BIBLIOGRAFÍA

American Banker. (2024, August 1). *Poor testing allowed CrowdStrike error to crash millions of computers. American Banker. Retrieved from https://www.americanbanker.com*

Wikipedia. (2024). *2024 CrowdStrike incident. In Wikipedia. Retrieved from https://en.wikipedia.org/wiki/2024_CrowdStrike_incident*

Security Boulevard. (2024, July 25). *Lessons learned from the CrowdStrike incident: Strengthening organizational resilience. Security Boulevard. Retrieved from https://securityboulevard.com*

World Economic Forum. (2024, July 24). *Global IT outage: Top cybersecurity news this month. World Economic Forum. Retrieved from https://www.weforum.org*

AHA News. (2024, July 25). *CrowdStrike posts preliminary post-incident report on recent global IT outage. AHA News. Retrieved from https://www.aha.org/new*

Baylis, J., & Wirtz, J. J. (Eds.). (2011). *Introducción: La estrategia en el mundo contemporáneo. En The Globalization of World Politics: An Introduction to International Relations (6th ed.). Oxford University Press.*

van Tilborg, H. C. A., & Jajodia, S. (Eds.). (2011). *Encyclopedia of Cryptography and Security. Springer, Boston, MA.*