MINISTERIO DE DEFENSA NACIONAL

COMANDO GENERAL DE LA FUERZAS MILITARES

ESCUELA SUPERIOR DE GUERRA “GENERAL RAFAEL REYES PRIETO”

MY. BETANCOURT RUIZ DIEGO

MY. BUITRAGO LOZANO DIEGO

MY. CERQUERA PASTRANA LIBARDO

MY. CABEZAS CABEZAS MANUEL

DOCENTE

DR. JAIDER OSPINA NAVAS

ASIGNATURA

HABILIDADES PRÁCTICAS EN EL CIBERESPACIO

BOGOTÁ D.C

31 DE JULIO DE 2024

INCIDENTE DE CROWDSTRIKE

El incidente de CrowdStrike del 19 de julio de 2024 fue un evento de interrupción global significativo que afectó a usuarios de Microsoft Windows en todo el mundo. La causa principal fue un **error lógico** en una actualización de configuración de sensor de rutina enviada por CrowdStrike, una empresa de ciberseguridad. Este error desencadenó una pantalla azul de la muerte (BSOD) en sistemas críticos, causando interrupciones generalizadas en operaciones comerciales y servicios.

Cronología del Incidente:

1. **19 de julio, 04:09 UTC:** CrowdStrike envía una actualización de configuración de sensor de rutina a los sistemas Windows.
2. **Horas posteriores:** Los sistemas Windows comienzan a experimentar BSOD debido al error lógico en la actualización.
3. **CrowdStrike reconoce el problema:** La empresa identifica el problema y comienza a trabajar en una solución.
4. **CrowdStrike lanza una solución:** Se proporciona una solución a los clientes afectados para mitigar el problema.
5. **Días posteriores:** Los sistemas afectados se recuperan gradualmente a medida que se implementa la solución.

Análisis del Incidente:

El incidente de CrowdStrike destaca varios puntos críticos en la gestión de actualizaciones de software y la ciberseguridad:

- **Pruebas rigurosas:** La importancia de realizar pruebas exhaustivas antes de implementar actualizaciones en entornos de producción.
- **Planes de contingencia:** La necesidad de contar con planes de contingencia sólidos para responder a incidentes de manera rápida y efectiva.
- **Comunicación transparente:** La importancia de una comunicación transparente con los clientes y las partes interesadas durante un incidente.

Lecciones Aprendidas:

- **Validación de actualizaciones:** Implementar procesos de validación más rigurosos para actualizaciones de software crítico.
- **Automatización de pruebas:** Utilizar herramientas de automatización para realizar pruebas exhaustivas antes de la implementación.
- **Monitorización en tiempo real:** Implementar sistemas de monitorización en tiempo real para detectar y responder a problemas de manera rápida.
- **Comunicación proactiva:** Establecer canales de comunicación claros y proactivos con los clientes durante incidentes.

Acciones de Remediación:

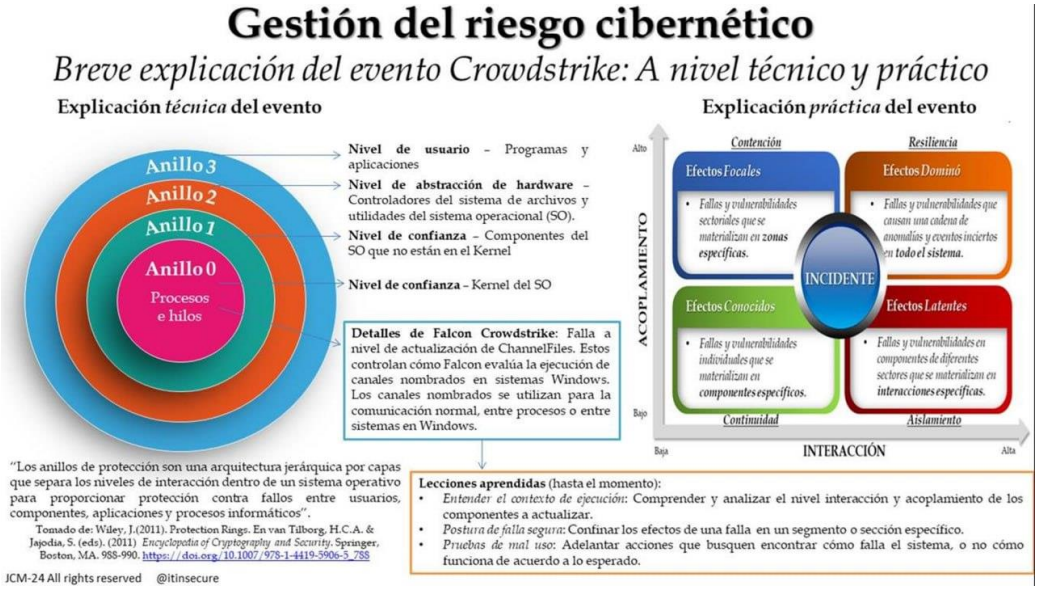
- **Revisión de procesos de actualización:** CrowdStrike ha revisado y mejorado sus procesos de prueba y validación de actualizaciones.
- **Fortalecimiento de la monitorización:** Se han implementado sistemas de monitorización más robustos para detectar anomalías en tiempo real.
- **Mejora de la comunicación:** Se han establecido canales de comunicación más efectivos para mantener a los clientes informados durante incidentes.

El incidente de CrowdStrike sirve como un recordatorio de la importancia de la ciberseguridad y la gestión de riesgos en el mundo digital. Las empresas deben tomar medidas proactivas para proteger sus sistemas y datos, y estar preparadas para responder a incidentes de manera efectiva.

Las fuentes de información:

- **LISA News:** Las consecuencias económicas del incidente de CrowdStrike: https://www.lisanews.org/ciberseguridad/las-consecuencias-economicas-del-incidente-de-crowdstrike/
- **Cointelegraph:** Opinión de analistas: la vulnerabilidad de las criptomonedas ante el incidente de CrowdStrike: https://es.cointelegraph.com/news/crowdstrike-blackout-impact-crypto-firms

EXPLICACIÓN DE SLIDE



La imagen presenta un análisis del incidente de CrowdStrike desde una perspectiva técnica y práctica, utilizando el modelo de anillos de protección como marco de referencia.

Anillos de Protección:
Los anillos de protección son un mecanismo de seguridad que divide un sistema operativo en niveles jerárquicos, donde el anillo 0 es el más privilegiado (núcleo del sistema) y el anillo 3 el menos privilegiado (aplicaciones de usuario). Esta arquitectura busca aislar los componentes del sistema y limitar el impacto de fallos.

Explicación Técnica:
El fallo de CrowdStrike se originó en una actualización de los ChannelFiles de Falcon, un componente situado en el anillo 0. Estos archivos controlan cómo Falcon (software de seguridad de CrowdStrike) evalúa la ejecución de canales nombrados en Windows, un mecanismo de comunicación esencial entre procesos y sistemas. El error en la actualización provocó un fallo en cascada que afectó a sistemas en todos los anillos, generando la pantalla azul de la muerte (BSOD) y la interrupción de servicios.

Explicación Práctica:
Desde una perspectiva práctica, el fallo se manifestó en la interrupción de programas y aplicaciones (anillo 3), afectando a usuarios finales y generando efectos focales (problemas específicos) y efectos dominó (cadenas de anomalías en todo el sistema).