Caso práctico 3:

1.Preparación:

Los roles del equipo de respuesta serian:

- **Líder de equipo:** Responsable de coordinar todas las actividades de respuesta al incidente, tomar decisiones clave y asegurar una comunicación efectiva dentro del equipo y con la dirección.
- **Analista de seguridad:** Monitorea y analiza la actividad sospechosa, identifica vulnerabilidades y proporciona recomendaciones técnicas para la contención y mitigación del incidente.
- **Especialista en redes**: Encargado de analizar el tráfico de red para identificar vectores de ataque, contener la propagación del incidente, y asegurar la infraestructura de red.
- **Especialista en Sistemas:** Responsable de la seguridad y la integridad de los sistemas operativos y aplicaciones afectadas.
- **Equipo Legal y de Cumplimiento:** Asegura que todas las acciones de respuesta al incidente cumplan con las normativas y regulaciones aplicables. También maneja la notificación a las autoridades y a las partes interesadas.
- **Oficial de Comunicaciones:** Gestiona la comunicación interna y externa, asegurando que la información se transmita correctamente dentro de la organización y, si es necesario, al público o a los clientes.

Los canales de comunicación interna para reportar incidentes que utilizaría serian, un correo electrónico seguro, chat en tiempo real (Microsoft Teams), Línea telefónica segura, sistema de gestión de incidentes. Y los pasos a seguir

- **Documentación del plan de gestión de incidentes:**
- **Políticas de Respuesta a Incidentes:** Procedimientos detallados para cada etapa de la respuesta, roles y responsabilidades, y protocolos de escalamiento.
- **Guía de Comunicación:** Directrices sobre cómo y cuándo comunicar incidentes a las partes interesadas internas y externas.
- **Plantillas de Informes:** Para garantizar que la documentación de los incidentes sea uniforme y cumpla con las regulaciones.

2.Descripción del incidente de seguridad detectado: Se detectó una actividad inusual en los servidores de FinTech, donde múltiples intentos de autenticación fallidos fueron seguidos por un acceso exitoso desde una dirección IP desconocida. Además, se observó un aumento significativo en el tráfico de datos hacia una ubicación externa, lo que sugiere un posible intento de extracción de datos.

Notificación del incidente: El analista de seguridad que detectó la actividad notificó inmediatamente al Líder del Equipo de Ciberseguridad mediante el sistema de gestión de incidentes. Paralelamente, se envió una alerta a través del chat en tiempo real a todos los

miembros del equipo de respuesta. El equipo legal y de cumplimiento fue notificado para asegurar que las acciones cumplan con las regulaciones aplicables.

3. Evaluación inicial del incidente: El incidente se evaluó como un posible acceso no autorizado con la intención de extraer datos sensibles de los clientes de FinTech. El análisis preliminar sugiere que el acceso fue logrado después de varios intentos de autenticación fallidos, lo que podría indicar un ataque de fuerza bruta.

Clasificación del incidente: El incidente se clasifica como de alta gravedad debido al riesgo de pérdida de datos sensibles y al posible impacto en la reputación de la empresa. La prioridad de la respuesta es alta, y el nivel de impacto se considera crítico para las operaciones y la confianza de los clientes.

4. Como medidas inmediatas para contener y mitigar el incidente se procederá a la desconexión del servidor comprometido, bloqueo de IP, revocación de credenciales, activación de auditoría. Estas acciones limitarán la capacidad del atacante para extraer más datos y mitigarán la propagación del incidente a otros sistemas críticos dentro de la red de FinTech.

5. Investigación y análisis

Para investigar el incidente revisaría los Logs de seguridad, analizaría el tipo de malware y lo eliminaría del sistema además de entrevistarme con el personal que tenia acceso al sistema para descartar un ataque interno. Cómo métodos principales para realizar este proceso utilizaría el análisis de memoria para identificar procesos maliciosos y archivos ocultos y consultaría las bases de datos de amenazas conocidas.

6. Notificación y divulgación

Se notificaría el incidente a las Autoridades financieras y de protección de datos, además de a los clientes afectados y a la dirección de la empresa. La notificación incluirá detalles del incidente, los tipos de datos afectados, las medidas de contención tomadas, y los pasos que se están dando para mitigar los riesgos. Además, se proporcionará información sobre cómo los afectados pueden protegerse, como el cambio de contraseñas o la vigilancia de sus cuentas.

7. Recuperación y mejoras

Para recuperar los sistemas afectados se restaurarían los sistemas a copias de seguridad verificadas y se mejorarían las configuraciones de seguridad, además de hacer pruebas de penetración y evaluaciones de seguridad. Adicionalmente se implementaría una autenticación multifactor, un monitoreo continuo y se haría una revisión de las políticas de acceso.

8. Lecciones aprendidas

De este incidente se puede aprender la importancia de la detección temprana y la necesidad de fortalecer los controles de acceso. Estas lecciones se documentarán con un informe detallado del incidente y reuniones internas para actualizar las políticas de seguridad de la empresa.

Referencias:

Evitando la fuga de información en SCI. (s/f). Incibe.es. Recuperado el 12 de agosto de 2024, de https://www.incibe.es/incibe-cert/blog/evitando-fuga-informacion-sci

Gestión de incidentes de ciberseguridad. (s/f). Ikusi.com. Recuperado el 12 de agosto de 2024, de https://www.ikusi.com/mx/blog/gestion-de-incidentes-de-ciberseguridad-paso-a-paso/

Kriptos. (2024, febrero 28). *Ciberseguridad para servicios financieros: protegiendo sus activos y clientes*. Linkedin.com. https://www.linkedin.com/pulse/ciberseguridad-para-servicios-financieros-protegiendo-sus-activos-dshje/

Roles en ciberseguridad: desde el CEO a los usuarios finales. (s/f). Incibe.es. Recuperado el 12 de agosto de 2024, de https://www.incibe.es/empresas/blog/roles-en-ciberseguridad-desde-el-ceo-los-usuarios-finales

Virtual Desk. (2021, marzo 18). *Ciberseguridad en la Administración Pública: análisis del ciberataque sufrido por el SEPE*. Virtual Desk. https://virtualdesk.es/ciberseguridad-en-administracion-publica-analisis-ciberataque-sepe/