Escenarios PagoCrypto

Contexto PagoCrypto es una fintech con presencia en América Latina que provee entre sus productos, una billetera virtual tradicional, una de crypto varios métodos de pago, la posibilidad de hacer trading de monedas e ingreso/extracción de dinero hacia cuentas bancarias. La forma de uso de sus clientes es con una cuenta personal y con aplicaciones nativas y web.

Escenario I: Uno de los principales problemas que está afrontando PagoCrypto es que recientemente se empezaron a ver muchas denuncias de fraude por retiro de dinero. Al entrar en detalle sobre estas denuncias se encuentra que los retiros fraudulentos son desde un mismo dispositivo web conocido por el usuario (es decir donde ya venía operando en el pasado). ● ¿Cuál podría ser la amenaza que esté detrás de este ataque? ● ¿Cómo podríamos confirmar? ● ¿Qué iniciativas podríamos emprender para mitigar este problema? a corto/mediano/largo plazo?

Escenario II: ● ¿Qué otro tipo de amenazas podrían ser relevantes para el negocio de PagoCrypto? ● ¿Cómo podríamos anticiparnos a esas amenazas? ● ¿Qué iniciativas podríamos emprender para mitigar este problema? a corto/mediano/largo plazo?

Escenario III: Suponiendo que nos encontramos a fin/principio de año y teniendo en cuenta las amenazas de los problemas I y II. ● ¿Como plantearias la planificación del año para el equipo? Puede ser conceptual, en un listado, en una presentación, en un calendario... Como te parezca mejor. Aclaración: tenés libertad para asumir todos los supuestos que te hagan falta, siempre y cuando aclares que lo estás haciendo y puedas justificarlos.

Escenario I

Amenaza detrás del ataque

La amenaza más probable detrás de estos retiros fraudulentos desde un dispositivo web conocido podría ser un ataque de tipo **"Account Takeover" (ATO)**, donde los atacantes han obtenido acceso a las credenciales del usuario y están realizando transacciones sin su conocimiento. Esto puede suceder a través de:

1. **Phishing**: Los atacantes engañan al usuario para que revele sus credenciales.
2. **Malware**: Un software malicioso en el dispositivo del usuario que captura credenciales.
3. **Credential Stuffing**: Uso de combinaciones de usuario/contraseña filtradas de otros servicios.

Confirmación de la amenaza

Para confirmar este tipo de actividad fraudulenta, sería crucial realizar un análisis forense detallado de los registros de acceso, patrones de transacción, y comportamiento del usuario. Además, se podría investigar si hay vulnerabilidades en la autenticación o posibles brechas de seguridad en la aplicación web.

Para confirmar esta amenaza, podríamos:

1. **Revisión de logs**: Analizar los registros de acceso y transacciones para identificar patrones inusuales, como inicios de sesión sospechosos o transacciones fuera del comportamiento normal del usuario.
2. **Entrevistas con usuarios afectados**: Hablar directamente con los usuarios que han reportado fraudes para obtener más información sobre cualquier actividad inusual en sus cuentas.
3. **Análisis de dispositivos**: Realizar un análisis de seguridad en los dispositivos desde los cuales se realizaron las transacciones fraudulentas para detectar posibles malware.

Iniciativas para mitigar el problema

- **Corto plazo**:
  - Implementar autenticación multifactor (MFA) obligatoria.
  - Enviar alertas en tiempo real a los usuarios sobre actividades inusuales en sus cuentas.
  - Realizar campañas de concientización sobre phishing y prácticas de seguridad.
- **Mediano plazo**:
  - Fortalecer la detección de fraudes con sistemas de análisis de comportamiento que detecten actividades inusuales.
  - Implementar soluciones de seguridad avanzada como la detección y respuesta en endpoints (EDR).
  - Realizar auditorías de seguridad periódicas en la plataforma.
- **Largo plazo**:
  - Integrar inteligencia artificial para mejorar la detección de fraudes y amenazas en tiempo real.
  - Establecer alianzas con otras fintechs y organizaciones para compartir información sobre amenazas y mejores prácticas.

Escenario II

Otras amenazas relevantes

1. **Ataques de Denegación de Servicio (DDoS)**: Que podrían afectar la disponibilidad del servicio.
2. **Vulnerabilidades en la Aplicación**: Fallos en la seguridad del software que pueden ser explotados.
3. **Ataques internos**: Empleados malintencionados o negligentes que puedan causar brechas de seguridad.
4. **Ransomware**: Secuestro de datos críticos a cambio de un rescate.
5. **Regulaciones cambiantes:** Riesgos legales y de cumplimiento normativo en diferentes países de América Latina
6. **Fugas de información:** Compromiso de datos sensibles de usuarios o transacciones.

Anticipación a las amenazas

1. **Evaluaciones de riesgo**: Realizar evaluaciones periódicas de riesgo para identificar y priorizar posibles amenazas.
2. **Inteligencia de amenazas**: Utilizar servicios de inteligencia de amenazas para mantenerse informado sobre nuevas vulnerabilidades y tácticas de ataque.
3. **Simulaciones de ataques**: Realizar pruebas de penetración y ejercicios de simulación de ataques (red teaming) para identificar y corregir vulnerabilidades.
4. **Monitoreo continuo:** Implementar sistemas de detección temprana para ransomware y fugas de información.
5. **Actualizaciones regulatorias:** Mantener una sinergia constante con el equipo encargado de analizar las políticas regulatorias (Legales,Finanzas,Comex) para anticiparse y adaptar cualquier tipo de política de PagoCrypto en consecuencia.

Iniciativas para mitigar las amenazas

- **Corto plazo**:
  - Implementar firewalls y sistemas de prevención de intrusiones (IPS).
  - Capacitar a los usuarios en buenas prácticas de seguridad y concientización sobre ciberseguridad.
  - Realizar backups regulares y asegurar que los planes de recuperación ante desastres estén actualizados.
- **Mediano plazo**:
  - Implementar un programa de gestión de vulnerabilidades para identificar y corregir vulnerabilidades en el software.
  - Establecer un centro de operaciones de seguridad (SOC) para monitoreo y respuesta a incidentes (suponiendo que no existía este centro).
  - Desarrollar políticas y procedimientos de seguridad claros y efectivos.
- **Largo plazo**:
  - Integrar tecnologías de seguridad basadas en inteligencia artificial para la detección y respuesta automatizada a amenazas.
  - Realizar auditorías de seguridad y revisiones de cumplimiento normativo de forma regular.

Escenario III

Planificación anual para el equipo de ciberseguridad

Supuestos:

- El equipo cuenta con recursos suficientes y apoyo de la alta dirección.
- La planificación se alinea con los objetivos estratégicos de la empresa.
- Se tiene un equipo dedicado de ciberseguridad y un presupuesto asignado.

Plan anual

Q1 (Enero - Marzo):

- **Enero**:
  - Evaluación de riesgos y planificación estratégica del año.
  - Implementación de autenticación multifactor (MFA) obligatoria.
  - Iniciar campañas de concientización sobre ciberseguridad.
- **Febrero**:
  - Realizar auditorías de seguridad en todas las plataformas.
  - Implementar firewalls y sistemas de prevención de intrusiones (IPS), donde no existan, y/o actualizar/mejorar equipamiento y licenciamientos en consecuencia de aquellos equipos existentes.
- **Marzo**:
  - Capacitación del personal en buenas prácticas de seguridad.
  - Evaluar y actualizar el plan de recuperación ante desastres.

Q2 (Abril - Junio):

- **Abril**:
  - Implementar sistemas de análisis de comportamiento para detección de fraudes.
  - Establecer políticas de seguridad internas claras.
- **Mayo**:
  - Realizar pruebas de penetración y simulaciones de ataques.
  - Implementar soluciones de detección y respuesta en endpoints (EDR).
- **Junio**:
  - Establecer el centro de operaciones de seguridad (SOC).
  - Monitoreo continuo y ajustes según los resultados de las pruebas de penetración.

Q3 (Julio - Septiembre):

- **Julio**:
  - Integración de inteligencia de amenazas y actualización continua de sistemas de seguridad.
  - Fomentar una cultura de seguridad a través de programas internos.
- **Agosto**:
  - Realizar auditorías de seguridad externas.
  - Revisar y actualizar las políticas de seguridad y procedimientos.
- **Septiembre**:
  - Evaluar la efectividad de las medidas implementadas y realizar ajustes necesarios.
  - Desarrollar un plan de respuesta a incidentes mejorado.

Q4 (Octubre - Diciembre):

- **Octubre**:
  - Implementar tecnologías basadas en inteligencia artificial para detección y respuesta.

    - Realizar simulaciones de recuperación ante desastres.
- **Noviembre**:
    - Revisar el presupuesto y planificar necesidades para el próximo año.
    - Actualización de planes estratégicos basados en el análisis de amenazas.
- **Diciembre**:
    - Evaluación anual de todas las iniciativas y resultados obtenidos.
    - Planificación preliminar del próximo año y ajuste de estrategias.

Este plan está diseñado para asegurar una protección continua y proactiva contra amenazas de ciberseguridad, alineando las acciones con las necesidades del negocio y las mejores prácticas del sector.

Autor: Ing. Maximiliano Fochi

Fecha: 26-06-2024

Versión: V1