Ejercicio **Seguridad Informática Básica – Gpo. 2** **Fecha de entrega: 12 / 10/ 23**

Equipo 4 || Integrantes:

Castelan Ramos Carlos **317042711**

Martínez González Héctor Eduardo **316322122**

Martínez Sánchez Berenice Vianney **317581223**

Pineda González Rodrigo **317224397**

Vega Alvarez Marcos **420054432**

9

Con base en la poca información que puede obtenerse el escenario, emplee la psicología del intruso para detectar las 3 etapas de un ataque, explique DETALLADAMENTE cada una de las etapas reportando todo lo que el equipo detecte o supongo que sucedió y la forma en la que sucedió para que el ataque fuera exitoso y se realizara como se comenta en el texto siguiente

Escenario

El pasado 27 de febrero a las 9:10 de la mañana, cuando llegó el primer empleado del departamento de recursos humanos de la organización encontró que la puerta de la oficina había sido violada, de tal manera que los cajones de los archiveros habían sido saqueados, esto implicó notar que la carpeta con el nuevo proyecto había sido robada, varios documentos importantes se encontraron en el piso y lamentablemente estaban revueltos. Afortunadamente los equipos de cómputo se encontraron intactos. Sólo se reportaron, además de los papeles, un florero roto y una cafetera tirada en el piso.

La psicología del intruso se utiliza para analizar y entender las motivaciones, acciones y etapas que un intruso o atacante sigue durante un incidente. A continuación, analizaré las tres etapas de un ataque en el escenario proporcionado:

1) Preparación o planteamiento:

a) Objetivos:

- El objetivo del ataque es obtener información confidencial de la oficina de recursos humanos relacionado con el nuevo proyecto. Esto se evidencia por el robo de la carpeta con el nuevo proyecto y la búsqueda selectiva de documentos importantes.

b) Recursos humanos del ataque:

- El ataque potencialmente fue llevado a cabo por una persona o un grupo de personas que conocían la disposición de la oficina y sabían dónde encontrar información valiosa. Tenían conocimiento interno de la organización o acceso a información privilegiada.

c) Hora, fecha y lugar:

- El ataque tuvo lugar el 26 de febrero por la noche (un día antes) o por la madrugada del mismo día, un momento en el que la oficina estaba relativamente vacía y desprotegida o con poca

vigilancia, lo que sugiere que los atacantes escogieron deliberadamente este horario para minimizar las posibilidades de ser descubiertos. El lugar a atacar es la oficina de recursos humanos.

d) Diseño de plan(es):

- El ataque implicó la violación de la puerta de la oficina y el saqueo de los archiveros, lo que indica un plan premeditado. Los atacantes en el plan inicial lo hicieron de forma rápida, con apoyo de alguien que conoce las instalaciones y que conocía los horarios con menor concurrencia de gente, por lo que llegó de forma inmediata a la oficina de recursos humanos y forzó la puerta con una herramienta u instrumento, por lo que indica que el atacante conocía o se preparó para abrir puertas.

-Otros planes posibles pueden ser que la información obtenida sobre la organización se haya obtenido de manera no intencionada, pero en cualquier caso siempre fue a partir de una persona interna a la organización.

-Otra situación que se considera es que no se haya forzado la entrada, sino haya sido una situación para despistar y se haya podido entrar sin violar la puerta, así como también, entrar por algún otro acceso a la organización.

-Otra situación es que la persona se haya quedado en la empresa, e inclusive, que la carpete aún se encuentre dentro de la organización.

e) Recursos monetarios para realizar el ataque:

- Es difícil determinar los recursos monetarios utilizados en el ataque, pero los atacantes pueden haber invertido en herramientas o conocimientos técnicos para forzar la entrada de la oficina.

-O para sobornar a una persona interna a la organización o viceversa que una persona interna a la organización que quisiera el proyecto contratara a alguien para que lo robara.

f) Otros recursos que intervienen:

-Tiempo, el mínimo necesario para planear y realizar la actividad (25 minutos aproximadamente)

-Medios de transporte.

-Vestimenta (para disuadir).

-Telecomunicaciones.

g) Lo que se ganó/perdió en el ataque:

Lo que perdió la organización.

- Se perdió la carpeta con el nuevo proyecto, varios documentos importantes, un florero roto y una cafetera tirada en el piso.

2) Activación: Faltó más detalle en esta etapa

a) Acciones que disparan el ataque:

-Se activó debido al cierre de la institución.

-Seguramente gracias a la baja vigilancia o complicidad del guardia de seguridad.

-Conocimiento de la existencia, importancia y ubicación del proyecto. (Ubicación no exacta, solo saben en qué oficina)

3) Ejecución:

a) Ganancias que obtuvo el ataque:

- Los atacantes obtuvieron información confidencial de la organización, lo que podría ser valioso para competidores u otras partes interesadas.

-Posibilidad extorsionar a la organización.

b) Nivel de protección del bien:

- El nivel de protección de la oficina parece haber sido insuficiente, ya que los atacantes lograron violar la puerta y saquear los archiveros sin ser detectados.

-Los equipos de cómputo se encontraron intactos, lo que sugiere que los activos digitales podrían haber estado mejor protegidos en comparación con los documentos físicos.

-Mejorar o agregar un sistema de CCTV.

c) Intencionalidad del ataque:

- Es una acción completamente intencional, ya que se buscaba dañar a la empresa y obtener el proyecto mencionado.