¿Qué ataque recibimos?

Phishing.

Diagnostico: Al parecer recibimos un ataque de Phishing, donde un correo malintencionado se envió a un empleado que posteriormente abrió el correo que contenía dentro de sí un link. La máquina comenzó a tener comportamientos extraños.

La medida a tomar es contratar un experto en ciberseguridad para contrarrestar el impacto.

Paso 2: Analizar los logs del sistema para encontrar evidencia de actividad maliciosa.

Herramienta: Visores de sucesos. Para ver los logs. Actividades en el equipo y la red.

Con un visor de sucesos vimos intentos sospechosos hacía datos confidenciales de usuarios de alto nivel en la empresa.

Los antivirus también alertaron sobre comportamientos extraños. En este caso los datos a revisar serían alertas de malware detectado en el sistema por el antivirus.

Logs de Correo Electrónico (Email Logs)

Propósito: Detectar el correo malicioso que inició el ataque de phishing.

Datos clave a revisar:

Dirección de correo del remitente.

Asunto y contenido del correo.

Hora y fecha de recepción del correo.

Identificación de los enlaces dentro del correo y su destino.

Comportamiento del correo (por ejemplo, si intentó ejecutar algún script o descargar archivos).

Logs de Base de Datos

Propósito: Revisar si el atacante intentó acceder o extraer datos confidenciales.

Datos clave a revisar:

Consultas anormales hacia tablas sensibles (por ejemplo, tablas de usuarios o de pagos).

Accesos no autorizados a información privada o datos de clientes.

Modificaciones o eliminación de registros en bases de datos.

Paso 3: Determinar el Alcance del Compromiso y los Sistemas afectados

• Actividad: que se debe realizar cuando se identifica los sistemas comprometidos.

Revisar los sistemas interconectados: Desconectar el equipo comprometido de la red para evitar que el incidente se propague.

Evalúa el impacto en la infraestructura crítica: verificar que no se haya afectado y si se afectó seguir con las contramedidas.

3.2 Evaluación del Impacto:

Actividad: que se debe tener en cuenta para evaluar el impacto en la:

Disponibilidad: Se debe tener en cuenta si el sistema sigue siendo accesible, que está pasando en él, si está muy lento o no reacciona**.**

Integridad: Revisar que los datos no hayan sido manipulados o alterados por el atacante.

Confidencialidad: Examinar si hubo acceso no autorizado a datos confidenciales de los usuarios/empleados para posteriormente tomar medidas.

Paso 4: Proponer Medidas de Contención Inmediatas:

4.1 Medidas de contención Inmediatas:

• Actividad: qué medidas se pueden implementar para detener el ataque y prevenir una mayor propagación.

Desconectar sistemas comprometidos: Desconectar el equipo o los equipos que están comprometidos para evitar la propagación del ataque. Aislar los sistemas afectados de la red principal.

Actualización de Sistemas: Asegurarse de que todo el software utilizado esté en su versión más reciente para minimizar vulnerabilidades conocidas. Hay que instalar los últimos parches de seguridad en el software y hardware vulnerable.

Cambio de Credenciales: Implementar nuevos sistemas de acceso y tener contraseñas más seguras. Es decir, reiniciar todas las claves de acceso y contraseñas del sistema comprometido.

4.2 Plan de Recuperación:

Actividad: Desarrollar un plan para restaurar los sistemas afectados y volver a la operación normal.

Restauración desde Copias de Seguridad: Usar las copias de seguridad recientes para restaurar los sistemas comprometidos.

Monitorea y Validación: Monitorear que todo este de nuevo funcionando de manera óptima y validar que aún no haya malware en el sistema o cualquier tipo de actividad maliciosa.

Evaluación Post-Incidente: Realizar un análisis detallado para ir a la raíz del ataque, ir documentando todo para prevenir futuros ataques.

4.3 Comunicación:

Actividad: Determinar a quién se le debe informar sobre la situación, las medidas tomadas, y las siguientes etapas.

Se le debe informar a los directivos y usuarios afectados para que estén al tanto de lo sucedido. Contratar a expertos en ciberseguridad para que hablen con más seguridad de lo sucedido a los demás.

Transparencia: Proporcionar detalles del incidente y las acciones hechas para mitigar el ataque.