Análisis del informe del incidente - Ejemplo

Resumen	Esta mañana, una pasante informó al departamento de TI que no pudo iniciar sesión en su cuenta de red interna. Los registros de acceso indican que su cuenta ha estado accediendo activamente a los registros de la base de datos de clientes, a pesar de estar bloqueada. La pasante indicó que recibió un correo electrónico esta mañana pidiéndole que se dirija a un sitio web externo e inicie sesión con sus credenciales de red interna para recuperar un mensaje. Creemos que este es el método utilizado por un agente de amenaza para obtener acceso a nuestra red y base de datos de clientes. Otros/as empleados/as han advertido que faltan varios registros de clientes o que contienen datos incorrectos. Parece que no solo se expusieron los datos de las/los clientes a un agente de amenaza, sino que también se eliminaron o manipularon algunos datos.
Identificar	El equipo de gestión de incidentes auditó los sistemas, dispositivos y políticas de acceso involucrados en el ataque para identificar las brechas de seguridad o fugas de datos. El equipo descubrió que el inicio de sesión y la contraseña de una pasante fueron obtenidos por un agente de amenaza y utilizados para acceder a los datos de nuestra base de datos de clientes. Tras la revisión inicial, parece que algunos datos de clientes se eliminaron de la base de datos.
Proteger	El equipo ha implementado nuevas políticas de autenticación para prevenir futuros ataques: autenticación de múltiples factores (MFA), límite de solo tres intentos para el inicio de sesión y capacitación para todos/as los/las empleados acerca de cómo proteger las credenciales de inicio de sesión. Además, implementaremos una nueva configuración de firewall para protección e invertiremos en un sistema de prevención de intrusiones (IPS).
Detectar	Para detectar nuevos ataques de acceso no autorizados en el futuro, el equipo

	utilizará una herramienta de registro por firewall y un sistema de detección de intrusiones (IDS) para monitorear todo el tráfico entrante de Internet.
Responder	El equipo deshabilitó la cuenta de red de la pasante. Brindamos capacitación a pasantes y empleados/as sobre cómo proteger las credenciales de inicio de sesión en el futuro. Informamos a la alta dirección de este evento y se pondrán en contacto con nuestros/as clientes por correo para informarles sobre la filtración de datos. La administración también deberá informar a las fuerzas del orden y otras organizaciones según lo exijan las leyes locales.
Recuperar	El equipo recuperará los datos eliminados restaurando la base de datos de la copia de seguridad completa realizada la noche anterior. Hemos informado al personal de que cualquier información de clientes que se haya ingresado o cambiado esta mañana no se registraría en la copia de seguridad. Por lo tanto, deberán volver a ingresar esa información en la base de datos una vez que esta se haya restaurado desde la copia de seguridad.

Reflexiones/Notas: