Incidente análisis de informes

Resumen	Esta mañana, una pasante informó al departamento de TI que no podía iniciar sesión en su cuenta de red interna. Los registros de acceso indican que su cuenta ha estado accediendo activamente a registros en la base de datos de clientes, aunque no pueda acceder a esa cuenta. La pasante indicó que recibió un correo electrónico esta mañana pidiéndole que fuera a un sitio web externo para iniciar sesión con sus credenciales de red interna para recuperar un mensaje. Creemos que este es el método utilizado por un actor malicioso para obtener acceso a nuestra red y base de datos de clientes. Un par de empleados más han notado que faltan varios registros de clientes o contienen datos incorrectos. Parece que no solo los datos de los clientes quedaron expuestos a un actor malicioso, sino que algunos datos también fueron eliminados o manipulados.
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. El equipo descubrió que un atacante malicioso obtuvo el nombre de usuario y la contraseña de un pasante y los utilizó para acceder a los datos de nuestra base de datos de clientes. Tras la revisión inicial, parece que algunos datos de los clientes se eliminaron de la base de datos.
Proteger	El equipo ha implementado nuevas políticas de autenticación para evitar futuros ataques: autenticación multifactor (MFA), intentos de inicio de sesión limitados a tres intentos y capacitación para todos los empleados sobre cómo proteger las credenciales de inicio de sesión. Además, implementaremos una nueva configuración de firewall protector e invertiremos en un sistema de prevención de intrusiones (IPS).

Detectar	Para detectar nuevos ataques de acceso no autorizado en el futuro, el equipo utilizará una herramienta de registro de 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 del pasante. Brindamos capacitación a pasantes y empleados sobre cómo proteger las credenciales de inicio de sesión en el futuro. Informamos a la alta dirección de este evento y ellos se comunicarán con nuestros clientes por correo para informarles sobre la violación de datos. La dirección también deberá informar a las autoridades y otras organizaciones según lo exigen las leyes locales.
Recuperar	El equipo recuperará los datos eliminados restaurando la base de datos a partir de la copia de seguridad completa de anoche. Hemos informado al personal que cualquier información del cliente ingresada o modificada esta mañana no se registrará en la copia de seguridad. Entonces, necesitarán volver a ingresar esa información en la base de datos una vez que se haya restaurado desde la copia de seguridad de anoche.