## EsINFORME FINAL DEL INCIDENTE

**Resumen ejecutivo**

La organización experimentó un incidente de seguridad el 28 de diciembre de 2022 a las 7:20 p.m., PT, durante el cual una persona logró obtener acceso no autorizado a la información personal identificable (PII) y a la información financiera de los clientes. Aproximadamente 50.000 documentos de clientes se vieron afectados. Se estima que el impacto financiero del incidente fue de US$100.000 en costos directos y posibles pérdidas de ingresos. El incidente ya está cerrado y se llevó a cabo una investigación exhaustiva.

**Cronología**

Aproximadamente a las 3:13 p.m., PT, del 22 de diciembre de 2022, un empleado recibió un correo electrónico de una dirección de correo electrónico externa. El remitente afirmó haber robado datos de clientes de forma exitosa. A cambio de no divulgar los datos a foros públicos, solicitó un pago en criptomonedas de US$25.000. El empleado asumió que el correo electrónico era spam y lo eliminó.

El 28 de diciembre de 2022, el mismo empleado recibió otro correo electrónico del mismo remitente que incluía una muestra de la información de cliente robada y se exigía un pago más alto: US$50.000.

Ese mismo día, el empleado notificó al equipo de seguridad, que comenzó su investigación del incidente. Entre el 28 y el 31 de diciembre de 2022, el equipo de seguridad se concentró en determinar cómo se robaron los datos y el alcance del robo.

**Investigación**

El equipo de seguridad recibió la alerta y viajó al lugar para comenzar la investigación.

La causa del incidente se identificó como una vulnerabilidad en la aplicación web de comercio electrónico. Esta vulnerabilidad permitió al agente de amenaza realizar un ataque de navegación forzada y acceder a los datos de transacción del cliente al modificar el número de pedido incluido en la cadena de URL de una página de confirmación de compra. Esta vulnerabilidad permitió al atacante acceder a las páginas de confirmación de compra del cliente y así exponer sus datos, que fueron recopilados y exfiltrados por el atacante.

Después de confirmar la vulnerabilidad de la aplicación web, el equipo de seguridad analizó los registros de acceso a la aplicación web, que indicaron que el atacante accedió a la información de miles de páginas de confirmación de compra.

**Respuesta y remediación**

La organización colaboró con el departamento de relaciones públicas para divulgar la filtración de datos a sus clientes. Además, ofreció servicios gratuitos de protección de identidad a quienes fueron afectados por el incidente.

Luego de la revisión de los registros del servidor web asociado a cargo del equipo de seguridad, se determinó que la causa del ataque fue muy clara. Había una única fuente de registro que mostraba un volumen excepcionalmente alto de pedidos de clientes enumerados secuencialmente.

**Recomendaciones**

Para evitar que se repita en el futuro, estamos tomando las siguientes medidas:

* Realizar escaneos de vulnerabilidad de rutina y pruebas de penetración.
* Implementar los siguientes mecanismos de control de acceso:
  + Implementar “allowlisting” (lista blanca) para permitir el acceso a un conjunto específico de URL y bloquear automáticamente todas las solicitudes fuera de este rango de URL.
  + Asegurar que solo los usuarios autenticados tengan acceso autorizado al contenido.