Investigacion de Incidente de Phishing 2024-12-18 #5

Globe Sistemas - Av. Libertador Jardin America

REPORTE FINAL DEL INCIDENTE PHISHING

Resumen ejecutivo

El 28 de diciembre de 2022, a las 7:20 p. m., hora del Pacífico, la organización sufrió un incidente de seguridad durante el cual una persona pudo obtener acceso no autorizado a información personal identificable (PII) e información financiera de los clientes.

Aproximadamente 50 000 registros de clientes se vieron afectados. Se estima que el impacto financiero del incidente es de $100 000 en costos directos y posible pérdida de ingresos. El incidente ya está cerrado y se ha realizado una investigación exhaustiva.

Cronología

Aproximadamente a las 3:13 p. m., hora del Pacífico, el 22 de diciembre de 2022, un empleado recibió un correo electrónico de una dirección de correo electrónico externa. El remitente del correo electrónico afirmó que había robado con éxito los datos de los clientes.

A cambio de no divulgar los datos en foros públicos, el remitente solicitó un pago en criptomonedas de $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. Este correo electrónico incluía una muestra de los datos robados del cliente y una mayor demanda de pago de $50,000. Ese mismo día, el empleado notificó al equipo de seguridad, que comenzó su investigación sobre el 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 se desplazó al lugar para comenzar la investigación.

La causa raíz del incidente se identificó como una vulnerabilidad en la aplicación web de comercio electrónico. Esta vulnerabilidad permitió al atacante realizar un ataque de navegación forzada y acceder a los datos de transacciones del cliente modificando 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, exponiendo los datos del cliente, que luego el atacante recopiló y exfiltró.

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

Respuesta y solución

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

Después de que el equipo de seguridad revisó los registros del servidor web asociado, 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 futuras recurrencias, estamos tomando las siguientes medidas: Realizar análisis de vulnerabilidades y pruebas de penetración de rutina.

\*Implementar los siguientes mecanismos de control de acceso:

\*Implementar listas blancas para permitir el acceso a un conjunto específico de URL y bloquear automáticamente todas las solicitudes fuera de este rango de URL.

\*Asegurarse de que solo los usuarios autenticados tengan acceso autorizado al contenido.