CIBERSEGURIDAD PARA
PEQUEÑOS NEGOCIOS

SEGURIDAD DE LOS PROVEEDORES

Puede que su negocio tenga proveedores con acceso a su información delicada.

Asegúrese de que esos proveedores estén tomando las medidas necesarias para proteger sus propias computadoras y redes. Por ejemplo, ¿qué sucedería si su contable pierde su computadora portátil con toda su información financiera? ¿O si la red de un proveedor que está conectada con su red sufre un ataque? El resultado: los datos de su negocio y la información personal de sus clientes puede terminar en las manos equivocadas — lo cual pone en riesgo a su negocio y a sus clientes.

CÓMO MONITOREAR A SUS PROVEEDORES

Póngalo por escrito

Incluya disposiciones de seguridad en los contratos con sus proveedores, como por ejemplo, un plan para Wevaluar y actualizar los controles de seguridad debido a que en las amenazas cambian. No negocie las disposiciones de seguridad que son cruciales para su compañía.

Verifique el cumplimiento

Establezca procesos que le permitan confirmar que los proveedores cumplen sus reglas. No crea sólo en las palabras.

Haga cambios según sean necesarios

Las amenazas de seguridad cibernética cambian rápidamente. Asegúrese de que sus proveedores mantengan su seguridad actualizada.

APRENDA MÁS EN
FTC.gov/PequeñosNegocios

FEDERAL TRADE COMMISSION

Homeland Security

NIST National Institute of Standards and Technology
U.S. Department of Commerce

SBA U.S. Small Business Administration

CIBERSEGURIDAD PARA PEQUEÑOS NEGOCIOS

CÓMO PROTEGER SU NEGOCIO

Controle el acceso

Establezca controles en las bases de datos que contengan información delicada. Limite el acceso según lo que sea necesario que sepa cada proveedor, y sólo por la cantidad de tiempo que el proveedor lo necesite para hacer un trabajo.

Use un sistema de autenticación de múltiples factores

Exija una autenticación de múltiples factores para acceder a las áreas de su red que contengan información delicada. Esto requiere algunos pasos adicionales además de iniciar la sesión con una contraseña – como un código temporario en un teléfono inteligente o una llave que se inserta en una computadora.

Proteja su red

Exija contraseñas sólidas: por lo menos 12 caracteres con una combinación de números, símbolos y letras mayúsculas y minúsculas. Nunca reutilice las contraseñas, no las comparta y limite la cantidad de intentos incorrectos de inicio de sesión para restringir los ataques de predicción de contraseñas.

Salvaguarde sus datos

Use un sistema de codificación potente y correctamente configurado. Esto protege la información delicada en el proceso de transferencia y almacenamiento.

QUÉ HACER SI UN PROVEEDOR SUFRE UN INCIDENTE DE SEGURIDAD DE DATOS

Establezca contacto con las autoridades

Reporte el ataque de inmediato a su departamento de policía local. Si no están familiarizados con las investigaciones de compromisos de información, establezca contacto con su oficina local del FBI.

Confirme que el proveedor haga las reparaciones

Si su negocio decide seguir trabajando con ese proveedor, asegúrese de que repare las vulnerabilidades y le garantice que su información estará protegida en el futuro.

Notifique a los clientes

Si sus datos o la información personal quedó comprometida, asegúrese de notificar a las partes afectadas ya que podrían estar en riesgo de un robo de identidad. Busque información sobre cómo hacerlo en *Data Breach Response: A Guide for Business* (disponible en inglés).

APRENDA MÁS EN FTC.gov/PequeñosNegocios

FEDERAL TRADE COMMISSION

Homeland Security

NIST National Institute of Standards and Technology U.S. Department of Commerce

SBA U.S. Small Business Administration