CIBERSEGURIDAD PARA
PEQUEÑOS NEGOCIOS

RANSOMWARE

Una persona de su compañía recibe un email.

Parece legítimo – pero con sólo hacer clic en un enlace o descargar un archivo adjunto, todo queda bloqueado fuera de su red. Desde ese enlace se descargó un programa que le secuestra sus datos como rehén. Eso es un ataque de un programa de rescate o ransomware.

Los atacantes le piden dinero o una cripto-moneda, pero aunque les pague, usted no sabe si los ciber-delincuentes se quedarán con sus datos o destruirán sus archivos. Mientras tanto, la información que necesita para operar su negocio y los datos delicados de sus clientes, sus empleados y su compañía están ahora en las manos de delincuentes. El ataque de ransomware puede tener un costo muy alto para su negocio.

CÓMO OCURRE

Los delincuentes pueden iniciar un ataque de ransomware de varias maneras.

Mensajes electrónicos fraudulentos
con enlaces y archivos adjuntos que ponen en riesgo sus datos y su red. Estos emails phishing son el origen de la mayoría de los ataque de programas de rescate o ransomware.

Sitios web infectados
que descargan automáticamente programas maliciosos en su computadora.

Vulnerabilidades del servidor
que pueden ser explotadas por los piratas informáticos.

Anuncios en línea
que contienen un código malicioso – incluso en sitios web conocidos y en los que confía.

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

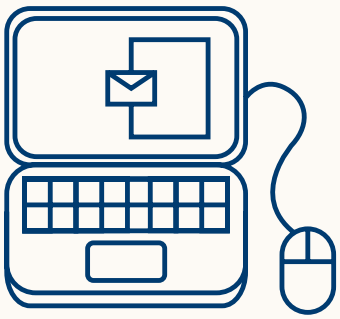
Implemente un plan
¿Cómo hará su negocio para mantenerse en pie y seguir operando después de un ataque de ransomware? Ponga el plan por escrito y compártalo con todo aquel que necesite conocerlo.

Haga copias de seguridad de sus datos
Guarde lo archivos importantes con regularidad en un disco externo o servidor que no esté conectado a su red. Haga copias de seguridad de datos como parte de sus operaciones comerciales de rutina.

Mantenga actualizada su seguridad
Instale siempre los parches de seguridad y actualizaciones más recientes. Busque otros medios de protección, como la autenticación de email y programas de prevención de intrusión, y configúrelos para que se actualicen automáticamente en su computadora. Es posible que tenga que hacerlo manualmente en los dispositivos móviles.

Alerte a su personal
Enséñeles cómo evitar las estafas de phishing y muéstreles algunas de las maneras más comunes en que se infectan los dispositivos y las computadoras. Incluya consejos para detectar los ataques de programas de rescate y protegerse contra ellos en sus sesiones regulares de capacitación y en sus comunicaciones.

QUÉ HACER SI LO ATACAN



Limite los daños
Desconecte inmediatamente de su red todas las computadoras o dispositivos infectados. Si le robaron sus datos, tome medidas para proteger a su compañía y notifique a aquellos que podrían estar afectados.

Mantenga su negocio en funcionamiento
Ahora es el momento de implementar ese plan. Tener copias de seguridad de sus datos lo ayudará.

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.

¿Debería pagar el rescate?
Las autoridades no lo recomiendan, pero es usted quien debe determinar si los riesgos y costos de pagar justifican la posibilidad de recuperar sus archivos. Sin embargo, es posible que el pago del rescate no le garantice la recuperación de sus datos.

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