Trend Micro

PROTECCIÓN CONTRA EL RANSOMWARE PARA SU NEGOCIO

El ransomware es implacable y los ataques que pueden devastar su negocio van en aumento

Es importante asegurarse de que está protegido para evitar la interrupción del negocio y el daño a su reputación como resultado de un ataque de ransomware, así como el impacto directo en su cuenta de resultados.

Asegurar la mejor protección cuando se tiene tiempo, presupuesto y otros recursos, puede parecer un desafío insuperable. También es difícil de entender cómo y dónde es más probable que un ataque de ransomware se produzca, ya que se trata de una amenaza que evoluciona rápidamente.

MINIMIZAR EL RIESGO

Cuento se trata de ransomware es necesario tener un plan para minimizar el riesgo. No hay ninguna poción mágica, pero entender las formas más comunes de ataque de ransomware permite establecer los pasos prioritarios que se pueden dar para dotar de la mejor protección para su negocio.

Protección del email

Protección del endpoint

Nuestras soluciones protegen su negocio en cada punto de entrada, por lo que no tiene que poner un precio a sus datos.

¿QUÉ ES EL RANSOMWARE?

El ransomware es un tipo de malware que bloquea, cifra o impide el acceso a los datos y sistemas por parte de sus propietarios a cambio de que las víctimas paguen un rescate al criminal responsable del ataque a fin de poder recuperar el acceso.

Se distribuye principalmente a través de kits de exploits, patrones de ingeniería social y los correos de spam que se envían a un gran número de direcciones de correo electrónico. Cuando un destinatario abre un archivo adjunto malicioso o hace clic en un enlace comprometido, el malware se descarga en el sistema del usuario.

El temor a la pérdida de datos de valor incalculable puede empujar a los usuarios a pagar el rescate y, aunque finalmente paguen, el desbloqueo o la descodificación de los archivos nunca está garantizada.

PROTECCIÓN DEL CORREO ELECTRÓNICO

Todo comienza con los usuarios. Son los más vulnerables cuando se trata de ransomware – ya sea que caigan por un correo electrónico de phishing o haciendo clic en un enlace web malicioso. Trend Micro ha bloqueado más de 99 millones de amenazas de ransomware desde octubre de 2015, y el 99 por ciento de ellas se encontraba en correos electrónicos maliciosos o enlaces web. Bloqueando el ransomware en el gateway de correo electrónico, se impide que llegue a sus usuarios.

Trend Micro Hosted Email Security es un gateway de correo electrónico basado en la nube y que le protege del ransomware que llega a través de correos electrónicos de spear phishing o adjuntos maliciosos en emails. Esto elimina la preocupación de que los usuarios sean engañados al pinchar en algo que pueda ocasionar un ataque ransomware en su negocio.

No requiere la instalación y mantenimiento de hardware o software. Todas las amenazas de correo electrónico se mantienen completamente fuera de su red, ayudándole a recuperar tiempo para que el personal técnico se centre en su negocio, permitiéndole aumentar productividad del usuario final, el ancho de banda, el almacenamiento en el servidor de correo y capacidad de la CPU. Además, el equipo global de expertos de Trend Micro gestiona todas las revisiones, parches, actualizaciones y ajustes de las aplicaciones para optimizar continuamente la seguridad y el rendimiento.

Hosted Email Security :

- Detecta y bloquea el ransomware a través del escaneo de malware y evaluación del riesgo de archivos
- Ofrece protección avanzada de amenazas con análisis de malware en sandbox y documentos de detección de vulnerabilidades
- Utiliza reputación web para proteger contra los enlaces web en los correos electrónicos que son maliciosos

Lo mejor de todo, es que se encuentra alojado en la nube por Trend Micro, por lo que no necesita preocuparse de despliegues ni gestiones en las instalaciones físicas. Y está disponible en un paquete, **Worry-Free Services Advanced**, que también incluye protección del endpoint.

PROTECCIÓN DEL ENDPOINT

Trend Micro detectó el 99 por ciento de las amenazas de ransomware en mensajes de correo electrónico o enlaces de Internet. Esto aún deja un 1 por ciento que podría hacerse a través de su terminal. Trend Micro Worry-Free Services Advanced ofrece capacidades específicas que minimizan el riesgo del ransomware en los endpoints, incluyendo:

- **Monitorización del comportamiento** para conductas sospechosas asociadas con ransomware, como el cifrado rápido de múltiples archivos, por lo que el proceso de cifrado se puede detener de forma automática y aislar el endpoint antes de que el ransomware pueda extenderse y causar más daño a sus datos
- **Reputación web en tiempo real** para determinar si una URL es una vía de entrega conocida de ransomware

Worry-Free Services Advanced ofrece protección cloud del correo electrónico y el endpoint, y proporciona seguridad de nivel empresarial diseñada específicamente para su pequeña empresa, por lo que puede:

- Centrarse en su negocio y no en su infraestructura de seguridad –dado que se trata de un servicio basado en la nube, su seguridad se mantiene actualizada de forma automática, y no hay nada que gestionar en las instalaciones
- Hacer cumplir las políticas de seguridad a los empleados en cualquier lugar, incluso en las sucursales y en sus hogares.
- Disfrutar de precios asequibles con una cuota anual de suscripción.

Cuando el ransomware infecta su negocio puede acceder a cualquier dato al que un usuario comprometido en su compañía también tenga acceso. Puede llevar varias horas intentar recuperar los archivos perdidos siguiendo ristras de emails, con pocas esperanzas de recuperación. A medida que el ransomware evoluciona, las empresas necesitan estar al día de las amenazas. Asóciese con Trend Micro y obtenga soluciones que previenen y mitigan los daños causados por esta amenaza potencialmente devastadora.

Para más información, visite **trendmicro.com/small-business-ransomware**

Proteja su empresa del ransomware

- Aproveche las copias de seguridad y los procesos de recuperación automáticos
- Aplique parches de seguridad tan pronto como estén disponibles
- Eduque y forme a sus empleados para prevenir el email phishing
- Limite el acceso a la información crítica de negocio
- Refuerce su postura de seguridad con protección por capas contra el ransomware

Amenazas de ransomware conocidas

PowerWare – Este malware tiene la habilidad de enumerar todas las unidades lógicas, incluyendo las unidades asignadas a redes compartidas. Esto pone a la red al completo en riesgo y podría convertirse en una amenaza mayor para las empresas.

ETYA - Puede sobrescribir el registro de arranque maestro de un sistema afectado para bloquear a los usuarios. Las unidades infectadas reciben la notificación de rescate cuando arrancan el sistema y no pueden ir más allá. Se entrega a las víctimas a través de servicios de almacenamiento cloud legítimos.

KeRanger - Un malware cifrado que es el primer crypto-ransomware para Mac y se instala a través de una aplicación de intercambio de archivos de código abierto. Los creadores de malware utilizan un certificado desarrollado por una app para Mac que consigue pasar el Apple Gatekeeper, una función de seguridad que permite a los usuarios restringir las fuentes desde las que pueden instalar aplicaciones.

SAMAS (También conocido como SAMSAM) – El primer ransomware que tiene la capacidad de cifrar archivos a través de redes, amenazando la base de datos y las copias de seguridad almacenadas en red de una organización. Los usuarios de SAMAS son conocidos por localizar manualmente y eliminar las copias de seguridad de la red para obligar a las empresas a pagar el rescate.

Locky - busca y elimina Volume Shadow Copy, archivos de backup automáticos de Windows.

MAKTUBLOCKER - El método de cifrado de este ransomware es similar a la mayoría, su vector de infección es único. Se presenta en forma de correo electrónico con un nombre y una dirección de email, por lo que el correo aparentemente tiene nuestra confianza. Cuando se descarga el archivo adjunto, se activa el ransomware.

TREND MICRO™

Securing Your Journey to the Cloud